CHAPTER 7

WANs and Remote Connectivity

After reading this chapter and completing the exercises, you will be able to:

- Identify network applications that require WAN technology
- Describe a variety of WAN transmission and connection methods
- Identify criteria for selecting an appropriate WAN topology, transmission method, and operating system
- Understand the hardware and software requirements for connecting to a network via modem
- Install and configure remote connectivity for a telecommuting client

On the Job

As a consultant for a small networking firm, I was thrilled to have the chance to work on the implementation of a WAN for a large West Coast city. The city wanted to connect more than 40 locations, including a sports arena, seniors' center, bus terminal, and maintenance plant, plus its business offices, so as to centrally control all file sharing, messaging, and printing occurring within the city government. It also wanted to provide Internet access for its employees. Some of the locations were situated 20 miles from the city center.

Our team of consultants recommended a combination of T1 and ISDN technology. For some locations, such as the city transportation office, we used both a T1 and an ISDN backup to the central connecting point, the city government's headquarters. Although the city didn't want to pay for a full-mesh topology, we did create a partial-mesh WAN by providing alternate routes around critical links. For example, we implemented a 56-KB dial-up link from one government building to another that would carry traffic between the buildings in case one of the T1s failed. We placed all servers at the headquarters, which allowed the city's IT staff to centrally control security and account administration. Finally, we connected the city to an ISP using a fractional T1. As a result, the city government is completely and reliably networked.

James Furness
CSI Networks

Now that you understand the basic transmission media, network models, and networking hardware associated with local area networks (LANs), you need to expand that knowledge to encompass wide area networks (WANs). As you learned in Chapter 1, a WAN is a network that connects two or more geographically distinct LANs. You might assume that WANs are the same as LANs, only bigger. Although a WAN is based on the same principles as a LAN, including reliance on the OSI Model, its distance requirements affect its entire infrastructure. As a result, nearly all characteristics of a WAN differ from the characteristics of a LAN.

To understand the difference between a LAN and WAN, think of the hallways and stairs of your house as LAN pathways. These interior passages allow you to go from room to room. To reach destinations outside of your house, however, you need to use sidewalks and streets. These public thoroughfares are analogous to WAN pathways—except that WAN pathways are not necessarily public.

This chapter discusses the technical differences between LANs and WANs and describes in detail WAN transmission media and methods. It also notes the potential pitfalls in establishing and maintaining WANs. In addition, it introduces you to remote connectivity for LANs—a technology that, in some cases, can be used to extend a LAN into a WAN. Remote connectivity and WANs are significant concerns for organizations attempting to meet the needs of telecommuting workers, global business partners, and Internet-based commerce. To pass the Net+ certification exam, you must be familiar with the variety of WAN and remote connectivity options. You also need to understand the hardware and software requirements for dial-up networking.

WAN Essentials

As you know, a WAN traverses a large geographical area—connecting LANs across the city or across the nation. For example, a WAN might connect the headquarters of an insurance company in New York with its satellite insurance offices in Hartford, Dallas, and San Francisco. The individual geographic locations (Hartford, Dallas, San Francisco) are known as WAN sites. A **WAN link** is a connection between one WAN site (or point) and another site (or point). A WAN link is typically described as point-to-point—because it connects one site to only one other site. That is, it does not typically connect one site to several other sites, in the way that LAN hubs or switches connect multiple segments or workstations. Nevertheless, one location may be connected to more than one location by multiple WAN links. Figure 7-1 illustrates the difference between WAN and LAN connectivity.

On the one hand, WANs and LANs are similar in some fundamental ways. In general, both can use any of the protocols mentioned in Chapter 3. Also, both primarily carry digital data. Finally, WANs and LANs have a similar function: to enable communications between clients and hosts that are not directly attached to each other.

On the other hand, WANs use different transmission systems, topologies, and sometimes, media, than LANs do. LANs typically use internal cabling, such as coaxial or twisted-pair. In contrast, WANs typically send data over public communications links, such as the telecommunications backbone provided by local and long-distance telephone companies. For better throughput, an organization might lease a continuously available link through another carrier, such as an Internet service provider (ISP). This kind of connection is called a **dedicated** line. Unlike a dial-up connection, dedicated lines do not require a user to connect and disconnect for a specified period of usage. They come in a variety of types that are distinguished by their capacity and transmission characteristics. You will learn about technology that relies on dedicated WAN connections, such as DSL and T1, later in this chapter.

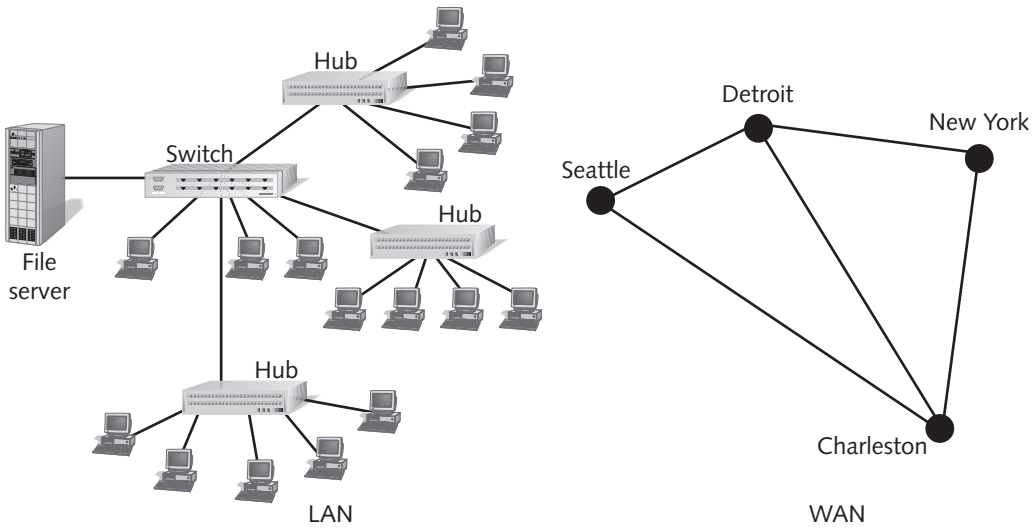

Figure 7-1 Differences in LAN and WAN connectivity

Chapter 5 introduced the various WAN topologies: star, ring, mesh, partial mesh, and hybrid. In that chapter, you learned that most WANs do not take the form of simple star or ring networks, but more likely employ mesh or partial-mesh configurations. As you know, the Internet is the largest WAN in existence today. Typically, the enterprise-wide WANs of individual organizations are conceived on a much smaller scale. For example, a WAN might begin by connecting only two offices (such as two branches of a bookstore chain that are located at either end of a city). As the organization grows, the WAN might grow to connect more and more sites, located across the city or around the world. Only an organization's information technology budget and aspirations limit the dimensions of its WAN.

Why might an organization need a WAN? Any organization that has multiple sites scattered over a wide geographical area needs a way to exchange data between those sites. Each of the following scenarios demonstrates a need for a WAN:

- A bank with offices around the state needs to connect those offices to gather transaction and account information into a central database.
- Regional sales representatives for a national pharmaceutical company need to dial in their sales figures and receive e-mail from headquarters.
- An insurance company allows parents on family leave to work from home by dialing into the company's network.
- An automobile manufacturer in Detroit contracts its plastic parts manufacturing out to a Delaware-based company. Through WAN links, the auto manufacturer can videoconference with the plastics manufacturer, exchange specification data, and even examine the parts for quality online.

- A support technician for the remote pharmaceutical salesperson may need to show the salesperson how to create a macro in an Excel spreadsheet. A remote control program, such as pcAnywhere, enables the support technician to "take over" the salesperson's PC (over a WAN link) and demonstrate how to create the macro.
- A clothing manufacturer sells its products over the Internet to customers throughout the world.

Although all of these businesses need WANs, they may not need the same kinds of WANs. Depending on the traffic load, budget, and geographical breadth, each might implement a different transmission method. For every business need, only a few (or possibly only one) appropriate WAN connection types may exist. However, many WAN technologies can coexist on the same network. As you learn about each technology, pay attention to its characteristics and think about its possible applications. To qualify for Net+ certification, you must be familiar with the variety of WAN connection types and be able to identify the types of networking environments that each suits best. You will learn about the various WAN transmission methods and connection types in the next section.

The WAN technologies discussed in the following section differ in terms of speed, reliability, cost, distance covered, and security. Also, some are defined by specifications at the Data Link layer, while others are defined by specifications at the Physical layer of the OSI Model. Both types of technology are included in this chapter because both types are used on WANs.

PSTN

PSTN, which stands for **Public Switched Telephone Network**, refers to the network of typical telephone lines and carrier equipment that service most homes. PSTN may also be called **plain old telephone service (POTS)**. It was originally composed of analog lines and developed to handle voice-based traffic. Now, however, most of the PSTN uses digital transmission through fiber-optic and copper twisted-pair cable, microwave, and satellite connections. This system is currently used for most dial-up connections to LANs. Indeed, for individuals simply picking up their e-mail or surfing the Web, PSTN is usually adequate. For example, a salesperson traveling to a conference might dial into her office's LAN from her hotel each night to pick up e-mail. So long as she doesn't have to download a significant amount of data, the throughput of her hotel room phone line connection would suffice.

A **dial-up** connection uses a PSTN or other line to access a remote server via modems at both the source (for example, the salesperson's computer) and destination (for example, the office LAN's server). As you have learned, a modem converts a computer's digital pulses into analog signals for the PSTN (because not all of the PSTN is necessarily capable of handling digital transmission), then converts the analog signals back into digital pulses at the receiving computer's end. Unlike other types of WAN connections, dial-up connections provide

a fixed period of access to the network, just as the phone call you make to a friend has a fixed length, determined by when you initiate and terminate the call. Ways to configure dial-up connections and establish remote connectivity are discussed in detail later in this chapter.

The advantages to using the PSTN are its ubiquity, ease of use, and low cost. A person can travel virtually anywhere in the world and have access to a phone line and, therefore, remote access to a network. Within the United States, the dial-up configuration for one location differs little from the dial-up configuration in another location. And nearly all mobile personal computers contain a modem, the only hardware a computer requires to establish this type of connection.

The disadvantage of the PSTN comes from its inability to ensure the quality or throughput required by many WAN applications. The quality of a WAN connection is largely determined by how many data packets that it loses or that become corrupt during transmission, how quickly it can transmit and receive data, and whether it drops the connection altogether. To improve this quality, most data transmission methods employ error-checking techniques. For example, TCP/IP depends on acknowledgments of the data it receives. In addition, many (though not all) PSTN links are now digital, and digital lines are more reliable than the older analog lines. Such digital lines reduce the quality problems that once plagued purely analog PSTN connections.

The more significant limiting factor of the PSTN is its capacity, or throughput. Currently, the most advanced PSTN modems advertise a connection speed of 56 Kbps. The 56-Kbps maximum is actually a *theoretical* threshold that assumes that the connection between the initiator and the receiver is pristine. Splitters, fax machines, or other devices that a modem connection traverses between the sender and receiver will all reduce the actual throughput. The number of points through which your phone call travels will also affect throughput. In addition, the **Federal Communications Commission (FCC)**, the regulatory agency that sets standards and policy for telecommunications transmission and equipment in the United States, limits the use of PSTN lines to 53 Kbps in order to reduce the effects of crosstalk. Thus, you will never actually achieve full 56-Kbps throughput using a modem over the PSTN.

To demonstrate how throughput diminishes over a PSTN connection, it's useful to follow a typical dial-up call from modem to modem, as pictured in Figure 7-2. Imagine you dial into your ISP to surf the Web through a 56-Kbps modem. You first initiate a call through your computer's modem. Your modem converts the digital signal from your computer into an analog signal that travels over the phone line to the local telephone company's **point of presence (POP)**. A POP is the place where the two telephone systems meet—either a long-distance carrier with a local telephone company, or a local carrier with an ISP's data center. At the POP, your signal is converted back to digital pulses and transmitted to your ISP's POP through a digital backbone (usually made of fiber-optic cable). The ISP's POP connects to its Internet service provider (the "larger ISP" in the figure) through a digital link, perhaps a T1 or T3 (discussed later in this chapter). Your request for information enters the Internet, and the transmission process is then reversed to bring you the desired Web page. Each time your transmission travels through

a POP, or is converted from analog to digital or digital to analog, it loses a little throughput. By the time the Web page returns to you, the connection may have lost from 5 to 30 Kbps, and your effective throughput might have been reduced to 30 Kbps or less.

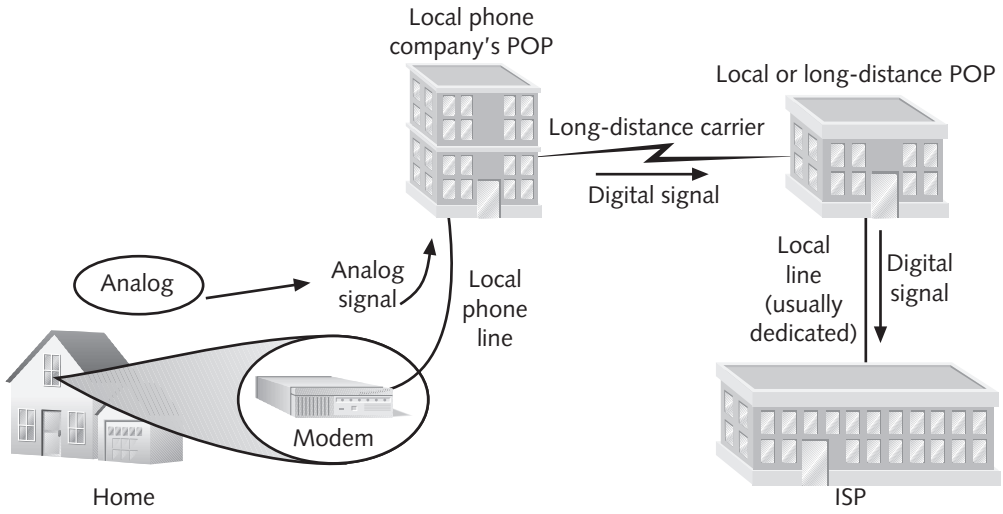

Figure 7-2 A typical PSTN connection to the Internet

"POP" is another network-related acronym that can have two completely different meanings, depending on its context. In this discussion of WAN and remote connectivity, a POP refers to a telecommunications service carrier's point of presence. In Chapter 11's in-depth discussion of TCP/IP protocols, POP will refer to the Post Office Protocol, used in e-mail transmission.

The PSTN uses circuit switching. (Recall from Chapter 5 that circuit switching is a means of transmitting data between two nodes with a dedicated point-to-point connection.) You might think that circuit switching makes the PSTN more secure than other types of WAN connections; in fact, the PSTN offers only marginal security. Granted, the PSTN is more secure than some forms of communication, such as cellular communications. Because it is a public network, however, PSTN presents many points at which communications can be intercepted and interpreted on their way from sender to receiver. For example, an eavesdropper could easily tap into the connection where your local telephone company's line enters your house. To make PSTN transmissions more secure, you must encrypt the data before it is sent. Chapter 15 describes data encryption techniques.

X.25 and Frame Relay

X.25 is an analog, packet-switched technology designed for long-distance data transmission and standardized by the ITU in the mid-1970s. The original standard for X.25 specified a maximum of 64-Kbps throughput, but by 1992 the standard was updated to include maximum throughput of 2.048 Mbps. It was originally developed as a more reliable alternative to the voice telephone system for connecting mainframe computers and remote terminals. X.25 ensures data reliability over long distances by verifying the transmission at every node. Unfortunately, this verification also renders X.25 comparatively slow and unsuitable for time-sensitive applications such as audio or video. X.25 was never widely adopted in the United States, but was accepted by other countries and was for a long time the dominant packet-switching technology used on WANs around the world.

Recall from Chapter 5 that, in packet switching, packets belonging to the same data stream may follow different, optimal paths to their destination. As a result, packet switching uses bandwidth more efficiently and allows for faster transmission than if each packet in the data stream had to follow the same path, as in circuit switching. Packet switching is also more flexible than circuit switching, because packet sizes may vary.

Frame relay is an updated, digital version of X.25 that also relies on packet switching. The name is derived from the fact that data is separated into frames, which are then relayed from one node to another without any verification or processing. Partially because it doesn't perform the same level of error detection that X.25 performs, frame relay supports higher bandwidth than X.25. It offers a maximum of either 1.544-Mbps or 45-Mbps throughput. It was standardized in 1984 and became popular in the United States and Canada for reliable long-distance WAN connections. However, frame relay is being replaced by newer, faster technologies. On networking diagrams, packet-switched networks such as X.25 and frame relay are depicted as clouds, as shown in Figure 7-3, because of the indeterminate nature of their traffic patterns.

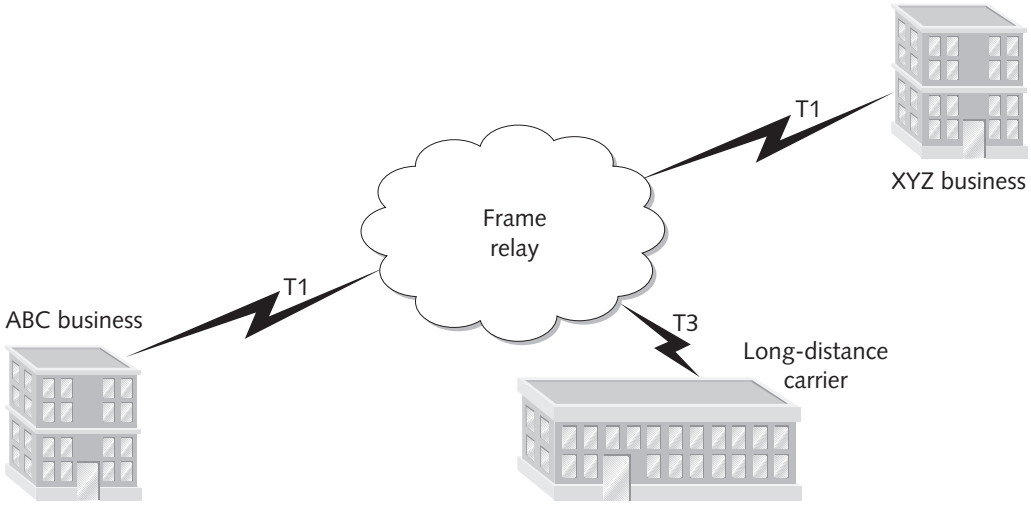

Figure 7-3 A WAN using frame relay

You may have seen the Internet depicted as a cloud on networking diagrams, similar to the frame relay cloud in Figure 7-3. In its early days, the Internet relied largely on X.25 or frame relay transmission—hence the similar illustration.

Both X.25 and frame relay may be configured as switched virtual circuits (SVCs) or more often, as permanent virtual circuits (PVCs). **SVCs** are connections that are established when parties need to transmit, then dismantled once the transmission is complete. **PVCs** are connections that are established before data needs to be transmitted and maintained after the transmission is complete. Note that in a PVC, the connection is established only between the two points (the sender and receiver); the connection does not specify the exact route the data will travel. Thus, in a PVC, data may follow any number of different paths to move from point A to point B. For example, a transmission traveling over a PVC from Baltimore to Phoenix might go from Baltimore to Washington, D.C., to Chicago, then to Phoenix; the next transmission over that PVC, however, might go from Baltimore to Boston to Chicago to Kansas City to Phoenix.

PVCs are *not* dedicated like T-carrier services. When you lease an X.25 or frame relay circuit from your local carrier, your contract reflects the endpoints you specify and the amount of bandwidth you require between those endpoints. The service provider guarantees a minimum amount of bandwidth, called the **committed information rate (CIR)**. Provisions usually account for bursts of traffic that occasionally exceed the CIR. When you lease a PVC, you share bandwidth with the other X.25 and frame relay users on the backbone. Most X.25 and frame relay circuits travel over T-carriers.

The advantage to leasing a frame relay circuit over leasing a dedicated service (such as a T1) is that you pay for only the amount of bandwidth required. Another advantage is

that frame relay is much less expensive than the newer WAN technologies offered today, such as ATM. Also, frame relay follows an established worldwide standard.

On the other hand, because frame relay and X.25 use shared lines, their throughput remains at the mercy of variable traffic patterns. In the middle of the night, data over your frame relay network may zip along at 1.544 Mbps; during midday, when everyone is surfing the Web, it may slow down to less than your CIR. In addition, frame relay circuits are not as private as dedicated circuits. Nevertheless, because they use the same connectivity equipment as T-carriers, they can easily be upgraded to T-carrier dedicated lines.

ISDN

ISDN (Integrated Services Digital Network) is an international standard, established by the International Telecommunications Union (ITU), for transmitting data over digital lines. ISDN uses the telephone carrier's lines and either a dial-up or dedicated connection. It is distinguished from PSTN by the fact that it relies exclusively on digital connections and by the fact that it can carry data and voice simultaneously. ISDN lines may carry as many as two voice calls and one data connection simultaneously. To achieve this feat, however, the ISDN user must have the correct devices to accept all three connections, as described later in this section. Through their ability to transmit voice and data simultaneously, ISDN lines can eliminate the need to pay for separate phone lines to support faxes, modems, and voice calls at one location. Local phone companies began offering ISDN in the mid-1980s, anticipating that the United States would convert to this all-digital system by the turn of the century. ISDN hasn't caught on as quickly as predicted, and other types of digital transmission methods now compete with it to serve customers who require moderate to fast throughput over phone lines.

All ISDN connections are based on two types of channels: B channels and D channels. The **B channel** is the "bearer" channel, employing circuit-switching techniques to carry voice, video, audio, and other types of data over the ISDN connection. A single B channel has a maximum throughput of 64 Kbps, although it is sometimes limited to 56 Kbps by the ISDN provider. As you will learn, the number of B channels in a single ISDN connection may vary. The **D channel** is the "data" channel, employing packet switching techniques to carry information about the call, such as session initiation and termination signals, caller identity, call forwarding, and conference calling signals. A single D channel has a maximum throughput of 16 Kbps. Each ISDN connection uses only one D channel.

In North America, two types of ISDN connections are commonly used: Basic Rate Interface (BRI) and Primary Rate Interface (PRI). A third type of ISDN connection, called Broadband ISDN (B-ISDN), was developed by the ITU in the late 1980s to provide more capacity than BRI or PRI. Today, organizations in need of the capacity offered by B-ISDN tend to choose newer, high-capacity lines, such as those using xDSL or T1 technology (both described later in this chapter).

BRI (Basic Rate Interface) uses two B channels and one D channel**,** as indicated by the following notation: 2B+D. The two B channels are treated as separate connections by the network and can carry voice and data or two data streams simultaneously and separate from each other. In a process called **bonding**, these two 64-Kbps B channels can be combined to achieve an effective throughput of 128 Kbps—the maximum amount of data traffic that a BRI connection can accommodate. Most consumers who subscribe to ISDN from home use BRI, which is the most economical type of ISDN connection.

Figure 7-4 illustrates how a typical BRI link supplies a home consumer with an ISDN link. (Note that the configuration depicted in Figure 7-4 applies to installations in North America only. Because transmission standards differ in Europe and Asia, different numbers of B channels are used in the standard ISDN connections in those regions.) From the telephone company's lines, the ISDN channels connect to a Network Termination 1 device at the customer's site. The **Network Termination 1 (NT1)** device connects the twisted-pair wiring at the customer's building with the ISDN terminal equipment via RJ-11 (standard telephone) or RJ-45 data jacks. The ISDN **terminal equipment (TE)** may include cards or standalone devices used to connect computers to the ISDN line (similar to a network adapter used on Ethernet or Token Ring networks).

So that the ISDN line can connect to analog equipment, the signal must first pass through a terminal adapter. A **terminal adapter (TA)** converts digital signals into analog signals for use with ISDN phones and other analog devices. (Terminal adapters are sometimes called ISDN modems, though they are not, technically, modems.) Typically, telecommuters who want more throughput than their analog phone line will afford choose BRI as their ISDN connection. For a home user, the terminal adapter would most likely be an ISDN router, such as the 800 series router from Cisco Systems, while the terminal equipment would be an Ethernet card in the user's workstation plus, perhaps, a phone.

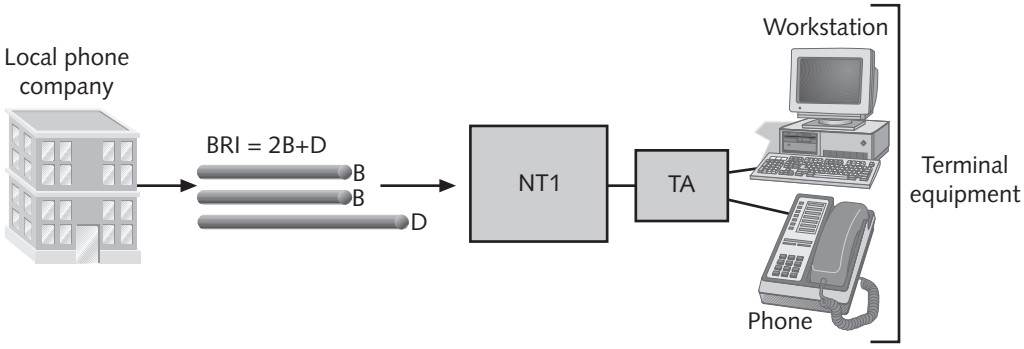

Figure 7-4 A BRI link

PRI (Primary Rate Interface) uses 23 B channels and one 64-Kbps D channel, as represented by the following notation: 23B+D. PRI is less commonly used by individual subscribers than BRI is, but it may be selected by businesses and other organizations that need more throughput. As with BRI, the separate B channels in a PRI link can

carry voice and data, independently of each other or bonded together. The maximum potential throughput for a PRI connection is 1.544 Mbps, the same as that for T1; in fact, PRI channels can be carried by T1 trunks.

PRI and BRI connections may be interconnected on a single network. PRI links use the same kind of equipment as BRI links, but require the services of an extra network termination device, called a **Network Termination 2 (NT2)**, to handle the multiple ISDN lines. Figure 7-5 depicts a typical PRI link as it would be installed in North America.

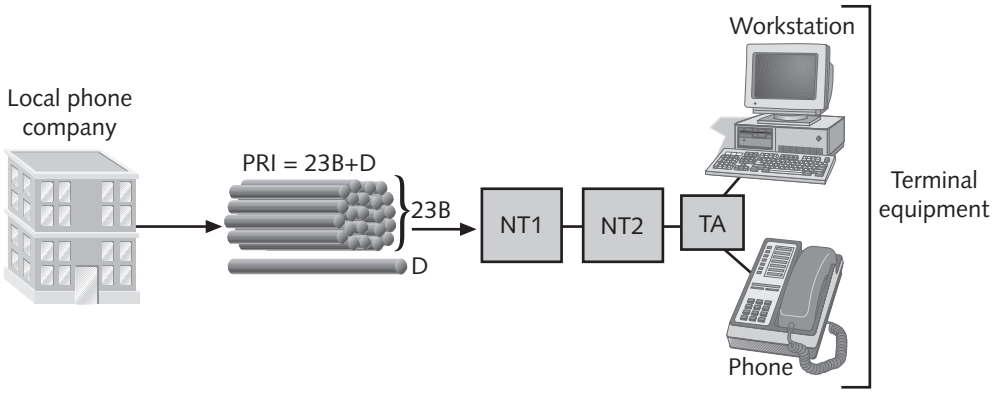

Figure 7-5 A PRI link

Individual customers who need to transmit more data than a typical modem can handle or who want to use a single line for both data and voice commonly use ISDN lines. ISDN, although not available in every location of the United States, can be purchased from most local telephone companies. The cost of using BRI averages $100 to $250 per month, depending on the customer's location. PRI and B-ISDN are significantly more expensive. In some areas, ISDN providers may charge customers additional usage fees based on the total length of time they remain connected.

One disadvantage of ISDN is that it can span a distance of only 18,000 linear feet before repeater equipment is needed to boost the signal. For this reason, it is only feasible to use for the **local loop** portion of the WAN link—that is, the part of a phone system that connects a customer site with a public carrier's POP.

T-CARRIERS

So far you have learned about WAN connections capable of relatively low throughput. Now you will learn about connections and transmission methods capable of 1.544-Mbps and higher throughput. Together, these transmission methods are known as **broadband** technologies. Note that this definition of broadband is different from the definition you learned in Chapter 4. Examples of this type of broadband technology are cable modem

services, DSL, and the group of connections that include T1s, fractional T1s, and T3s—collectively known as **T-carriers**. This section focuses on T-carrier technology. Subsequent sections cover DSL and cable modem technology.

T-carrier transmission uses time division multiplexing over two wire pairs (one for transmitting and one for receiving) to divide a single channel into multiple channels. For example, multiplexing enables a single T1 circuit to carry 24 channels, each capable of 64-Kbps throughput; thus a T1 has a maximum capacity of 24 × 64 Kbps, or 1.544 Mbps. Each channel may contain data, voice, or video signals.

AT&T developed T-carrier technology in 1957 in an effort to digitize voice signals, thereby enabling such signals to travel long distances. Before that time, voice signals, which were purely analog, were expensive to transmit over long distances because of the number of connectivity devices needed to keep the signal intelligible. In the 1970s, many businesses installed T1s to obtain more voice throughput per line. With increased data communication needs, such as Internet access and geographically dispersed offices, T1s have become common WAN links for use in medium to large businesses.

The next section describes the various types of T-carriers, then the chapter moves on to T-carrier connectivity devices.

Types of T-carriers

A number of T-carrier varieties are available to businesses today, as shown in Table 7-1. The most common T-carrier implementations are T1 and, for higher bandwidth needs, T3. A **T1** circuit can carry the equivalent of 24 voice or data channels, giving a maximum data throughput of 1.544 Mbps. A **T3** circuit can carry the equivalent of 672 voice or data channels, giving a maximum data throughput of 44.736 Mbps (its throughput is typically rounded up to 45 Mbps for the purposes of discussion).

The speed of a T-carrier depends on its signal level. The **signal level** refers to the T-carrier's Physical layer electrical signaling characteristics as defined by ANSI standards in the early 1980s. **DS0 (digital signal, level 0)** is the equivalent of one data or voice channel. All other signal levels are multiples of DS0.

You may hear signal level and carrier terms used interchangeably—for example, DS1 and T1. Technically, T1 is the North American implementation of the international DS1 standard. In Europe, the DS1 standard is implemented as E1 and offers a slightly higher throughput than T1.

Table 7-1 Carrier specifications

Signal Level	Carrier	Number of T1s	Number of Channels	Throughput (Mbps)
DS0	—	1/24	1	.064
DS1	T1	1	24	1.544
DS1C	T1C	2	24	3.152
DS2	T2	4	96	6.312
DS3	T3	28	672	44.736
DS4	T4	168	4032	274.176

As a networking professional, you are most likely to work with T1 or T3 lines. In addition to knowing their capacity, you should be familiar with their costs and uses. T1s are commonly used by businesses to connect branch offices or to connect to a carrier, such as an ISP. Telephone companies also use T1s to connect their smaller central offices. ISPs may use one or more T1s or T3s, depending on the provider's size, to connect to their Internet carriers.

Because a T3 provides 28 times more throughput than a T1, many organizations may find that a few T1s—rather than a single T3—can accommodate their throughput needs. For example, suppose a university research laboratory needed to transmit molecular images over the Internet to another university, and its peak throughput need (at any given time) was 10 Mbps. The laboratory would require seven T1s (10 Mbps divided by 1.544 Mbps equals 6.48 T1s). Leasing seven T1s would prove much less expensive for the university than leasing a single T3.

The cost of T1s varies from region to region. On average, a T1 might cost between $500 and $2000 to install, plus an additional $500 to $2000 per month in access fees. The longer the distance between the provider (such as an ISP or a telephone company) and the subscriber, the higher a T1's monthly charge. Charges for local T1s may be based on mileage, whereas costs for long distance T1s vary on a city-to-city basis. For example, a T1 between Houston and New York will cost more than a T1 between Washington, D.C., and New York. Similarly, a T1 from the western suburbs of Detroit to the city center will cost more than a T1 from the city center to a business three blocks away.

For organizations that do not need constant bandwidth, a dial-up ISDN solution may prove more cost-effective than a T1. For businesses that *do* need a dedicated circuit, but don't always need as much as 1.544-Mbps throughput, a fractional T1 is a better option. A **fractional T1** lease allows organizations to use only some of the channels on a T1 line and be charged according to the number of channels they use. Thus fractional T1 bandwidth can be leased in multiples of 64 Kbps. A fractional T1 is best suited to businesses that expect their traffic to grow and that may require a full T1 eventually, but can't currently justify leasing a full T1.

T3s are very expensive and are used by the most data-intensive businesses—for example, computer consulting firms that provide online data backups and warehousing for a number of other businesses or large long-distance carriers. A T3 is much more expensive than

even multiple T1s. It may cost as much as $3000 to install, plus monthly service fees based on usage. If a customer uses the full T3 bandwidth of 45 Mbps, for example, the monthly charges might be as high as $18,000. Of course, T3 costs will vary depending on the carrier, your location, and the distance covered by the T3. In any event, however, this type of connection is significantly more expensive than a T1. Therefore, only businesses with extraordinary bandwidth requirements should consider using T3s.

T-carrier Connectivity

The approximate costs mentioned previously include monthly access and installation, but not connectivity hardware. Every T-carrier line requires connectivity hardware at both the customer site and the local carrier's POP. Connectivity hardware may be purchased or leased. If your organization uses an ISP to establish and service your T-carrier line, you will most likely lease the connectivity equipment. If you lease the line directly from the local carrier and you anticipate little change in your connectivity requirements over time, however, you may want to purchase the hardware.

T-carrier lines require specialized connectivity hardware that cannot be used with other WAN transmission methods. In addition, T-carrier lines require different media, depending on their throughput. In this section, you will learn about the physical components of a T-carrier connection between a customer site and a local carrier.

Wiring

As mentioned earlier, the T-carrier system is based on AT&T's original attempt to digitize existing long-distance telephone lines. As a result, T1 technology can use unshielded or shielded twisted-pair copper wiring—in other words, plain telephone wire. Because the digital signals require a cleaner connection (that is, one less susceptible to noise and attenuation), however, shielded twisted-pair is preferable. For T1s using shielded twisted-pair, repeaters must regenerate the signal approximately every 6000 feet. Twisted-pair wiring cannot adequately carry the high throughput of multiple T1s or T3 transmissions. Thus, for multiple T1s, coaxial cable, microwave, or fiber-optic cabling may be used. For T3s, microwave or fiber-optic cabling is necessary.

CSU/DSU (Channel Service Unit/Data Service Unit)

Although CSUs (channel service units) and DSUs (data service units) are actually two separate devices, they are typically combined into a single box called a **CSU/DSU**. The CSU/DSU is the connection point for a T1 line at the customer's site. The **CSU** provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The **DSU** converts the digital signal used by bridges, routers, and multiplexers into the digital signal sent via the cabling. The CSU/DSU box connects the incoming T1 with the multiplexer, as shown in Figure 7-6.

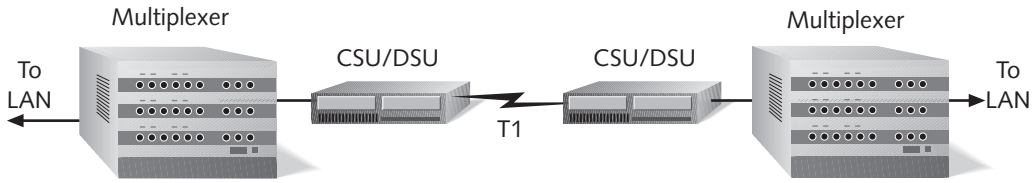

Figure 7-6 A CSU/DSU connecting a T1

Multiplexer

As you learned earlier, a multiplexer is a device that combines multiple voice or data channels on one line. The devices that connect to the multiplexer are collectively known as terminal equipment. Multiplexers can take input from a variety of terminal equipment, such as bridges, routers, or telephone exchange devices that accept only voice transmissions (such as a PBX system). Figure 7-7 depicts a typical use of a multiplexer with a T1-connected data network. In some network configurations, the multiplexer is integrated with the CSU/DSU. In the following sections, you will learn how routers and bridges integrate with CSU/DSUs and multiplexers to connect T-carriers to a LAN.

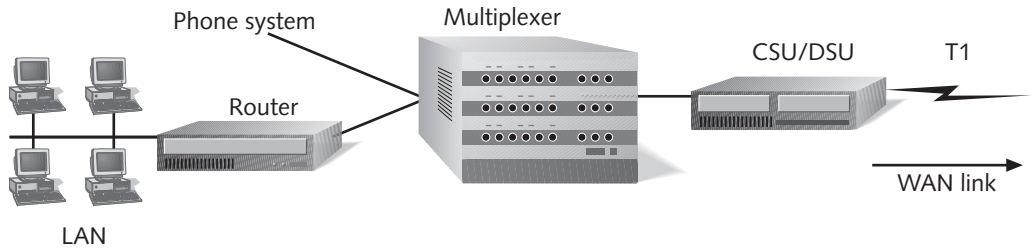

Figure 7-7 Typical use of a multiplexer on a T1-connected data network

Routers and Bridges

On a typical T1-connected data network, the terminal equipment will consist of bridges, routers, or a combination of the two. The bridges and routers used in this situation are identical to the bridges and routers you learned about in Chapter 6. With the T1 connection, the bridge or router would typically integrate two types of networks: the Internet and an Ethernet or Token Ring LAN at the customer's site. A router, which can convert TCP/IP to other protocols, is necessary if the internal LAN does not run TCP/IP. Figure 7-8 depicts the use of a router with a T1-connected network.

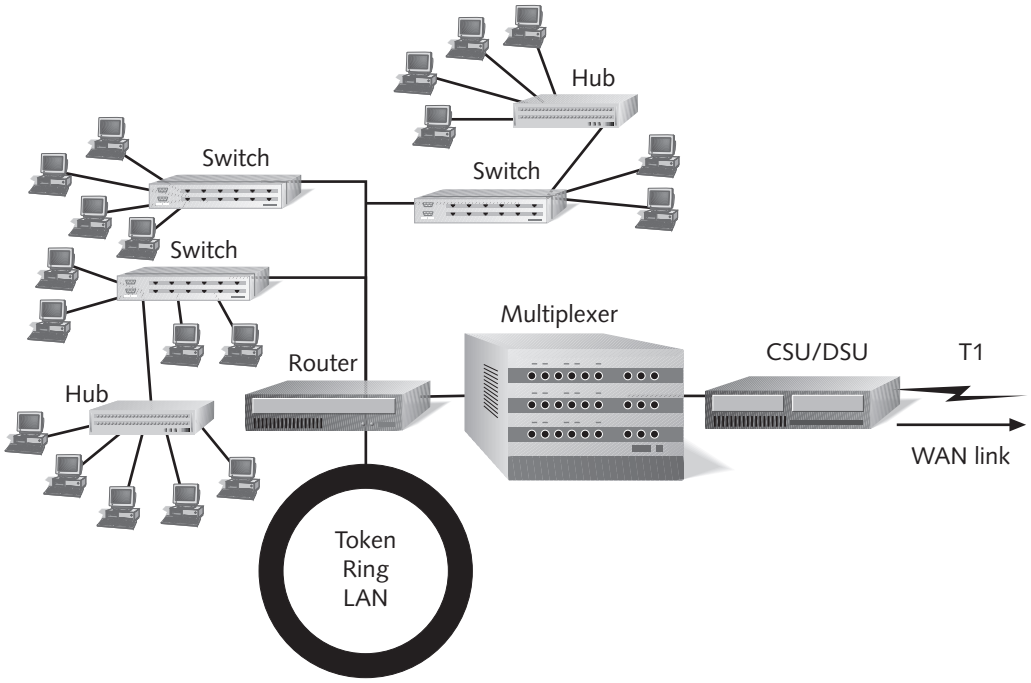

Figure 7-8 A router on a T1-connected network

DSL

Digital subscriber line (DSL) is a type of WAN connection introduced in the late 1990s that competes directly with ISDN and T1 services. Like ISDN, DSL can span only limited distances without the help of repeaters and is therefore best suited to the local loop portion of a WAN link. Also, like ISDN, DSL can support multiple data and voice channels over a single line.

DSL uses advanced data modulation techniques to achieve extraordinary throughput over regular phone lines. Recall from Chapter 4 that in data modulation, one signal alters the frequency, phase, or amplitude of another signal to enable multiple signals to traverse the same wire without interfering with each other. Depending on the type, DSL may use any one of these three types of modulation.

Many individuals and businesses are choosing DSL for its low cost, ease of installation, and high throughput. In most areas of the United States, a DSL connection that can supply nearly as much throughput as a T-1 costs less than $100 per month. Consumer-grade DSL, with approximately half as much bandwidth, can cost as low as $20 per month. Because it runs over existing telephone lines, DSL installation is relatively simple, requiring only a special modem and some configuration at the user end. Also, DSL is a dedicated service, which means a connection is always available for use. In the next section you will learn about the many varieties of DSL in use today.

Types of DSL

The term **xDSL** refers to all DSL varieties, of which at least eight currently exist. The better-known DSL varieties include Asymmetric DSL (ADSL), G.Lite (a version of ADSL), High Bit-Rate DSL (HDSL), Symmetric or Single-Line DSL (SDSL), and Very High Bit-Rate DSL (VDSL)—the "x" in "xDSL" is replaced by the variety name. DSL types can be divided into two categories: asymmetrical and symmetrical.

To understand the difference between these two categories, you must understand the concept of downstream and upstream data transmission. The term **downstream** refers to data traveling from the carrier's POP to the customer. The term **upstream** refers to data traveling from the customer to the carrier's POP. In some types of DSL, the throughput rates for downstream and upstream traffic differ. That is, if you were connected to the Internet via a DSL link, you might be able to pick up your e-mail messages more rapidly than you could send them because the downstream throughput is usually greater. A technology that offers more throughput in one direction than in the other is considered **asymmetrical**. In asymmetrical communications, downstream throughput is usually much higher than upstream throughput. Asymmetrical communication is well suited to users who pull more information off the network than they send to it—for example, people watching videoconferences or people surfing the Web.

Conversely, **symmetrical** technology provides equal capacity for data traveling both upstream and downstream. Symmetrical transmission is suited to users who both upload and download significant amounts of data—for example, a bank's branch office, which sends large volumes of account information to the central server at the bank's headquarters and in turn, receives large amounts of account information from the central server at the bank's headquarters. ADSL and VDSL are examples of asymmetrical DSL; HDSL and SDSL are examples of symmetrical DSL.

The types of DSL also vary in terms of their capacity and maximum line length. A VDSL line that carries as much as 52 Mbps in one direction and as much as 6.4 Mbps in the opposite direction can extend a maximum of 1000 feet between the customer's premises and the carrier's POP. This limitation might suit businesses located close to a telephone company's data center (for example, in the middle of a metropolitan area), but it won't work for most individuals. The most popular form of DSL, ADSL, provides a maximum of 8 Mbps in one direction and a maximum of 1.544 Mbps in the other direction; at its highest speeds, it is limited to a distance of 12,000 feet between the customer's premises and the carrier's POP. This distance (more than two miles) renders it suitable for most telecommuters. Table 7-2 compares current specifications for five DSL types.

Table 7-2 Comparison of DSL types

DSL Type	Maximum Upstream Capacity (Mbps)	Maximum Downstream Capacity (Mbps)	Distance Limitation (feet)
ADSL ("full rate")	1	8	18,000
G.Lite (a type of ADSL)	0.512	1.544	25,000
HDSL	1.544 or 2.048	1.544 or 2.048	12,000
SDSL	1.544	1.544	9,000
VDSL	1.6, 3.2, or 6.4	13, 25.9, or 51.8	1000 – 5000

In addition to their data modulation techniques, capacity, and distance limitations, DSL types vary according to how they use the PSTN. Following you will learn about how DSL connects to a business or residence over the PSTN.

DSL Connectivity

DSL connectivity, like ISDN, depends on the PSTN. To understand how DSL uses the PSTN, it is helpful to first understand that voice signals use a very small range of frequencies, between 0 and 35 KHz. This leaves higher, inaudible frequencies unused and available for carrying data. Some versions of DSL, such as the popular full-rate ADSL, G.Lite, and VDSL, use the same pair of wires that carry voice signals, but modulate data on the higher frequencies. In the case of full-rate ADSL, a splitter must be installed at the carrier and at the customer's premises to separate the data signal from the voice signal before it reaches the terminal equipment (for example, the phone or the computer). G.Lite, a slower and less expensive version of ADSL, eliminates the splitter but requires the use of a filter to prevent high-frequency DSL signals from reaching the telephone. This makes G.Lite easier to install. Other types of DSL, such as HDSL and SDSL, cannot use the same wire pair that is used for voice signals. Instead, these types of DSL use the extra pair of wires contained in a telephone cable (that are typically unused).

Once inside the customer's office or home, the DSL line must pass through a **DSL modem**, a device that demodulates the signal, extracting the information and passing it on to the computer. The DSL modem may also contain a splitter (for example, in the case of ADSL) to separate the line into multiple channels for voice and data signals. The DSL modem may be external to the computer and connect to a computer's Ethernet NIC via UTP cable or to the computer's USB port. Newer DSL modems come in the form of internal, PCI expansion boards. If the DSL bandwidth is to be shared on a LAN, the DSL modem could connect to a connectivity device, such as a hub or router, rather than to just one computer. Figure 7-9 represents a typical DSL connection, including its termination inside an office. Figure 7-10 depicts a DSL modem.

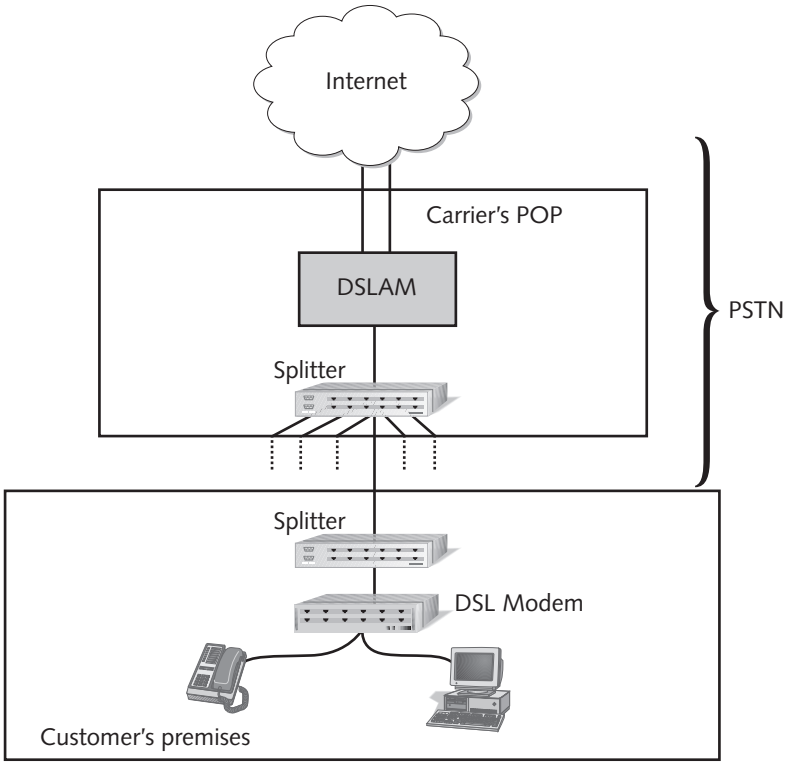

Figure 7-9 A DSL connection

Figure 7-10 A DSL modem

On the other end of the line, the DSL connection terminates at a carrier's POP. If necessary, a splitter is placed between the incoming line and the telephone and data switches. In order to accept the DSL signals, the carrier must have newer digital switching equipment. In areas of the country where carriers have not updated their switching equipment, DSL service is not available. Inside the carrier's POP, a device called a **DSL access multiplexer (DSLAM)** aggregates multiple DSL subscriber lines and connects them to a larger carrier or to the Internet backbone, as pictured in Figure 7-9.

As mentioned earlier, standards for DSL continue to evolve. Service providers and manufacturers have positioned DSL as a competitor for T1, ISDN, and cable modem services. The installation, hardware, and monthly access costs for DSL are similar to those for ISDN lines but are significantly less than the cost for T1s. Considering that DSL technology can provide faster throughput than T1s, it presents a formidable challenge to the T1 industry, especially given that T1s are typically too expensive for home users.

One drawback to DSL is that it is not available in all areas, and even where it is available, it may be subject to severe distance limitations. Another drawback is that DSL's relative newness (compared with ISDN and T1 technology, for example) has led to a backlog in DSL installations. Subscribers may wait a few months after ordering their DSL service before it can be installed. Add to that the fluctuating state of DSL standards and providers, and DSL appears to be a technology that will require some time to stabilize. Nevertheless, DSL has won over many consumers and small businesses who want more bandwidth than ISDN or PSTN can afford. As of 2000 over 2 million DSL lines were installed in the United States, and by some estimates that number is predicted to grow to over 23 million by 2004.

Cable

While local and long-distance phone companies race to make DSL the preferred method of Internet access for consumers, cable companies are pushing their own connectivity option, based on the coaxial cable wiring used for TV signals. Such wiring could theoretically transmit as much as 36 Mbps downstream and as much as 10 Mbps upstream. Thus cable is an asymmetrical technology. Realistically, however, cable will allow approximately 3 to 10 Mbps downstream and 2 Mbps upstream due to its shared nature (described later in this section) as well as bottlenecks that occur either at the Internet carrier's data facilities or on the Internet itself. The asymmetry of cable technology makes it a logical choice for users who want to surf the Web or download data from a network. Some companies are also developing services to deliver music, videoconferencing, and Internet services over cable infrastructure.

Cable connections require that the customer use a special **cable modem**, a device that modulates and demodulates signals for transmission and reception via cable wiring. Figure 7-11 provides an example of a cable modem. The cable modem then connects to a customer's PC via its USB port or through a UTP cable to a (typically Ethernet) NIC. Alternately, the cable modem could connect to a connectivity device, such as a hub or

router, to supply bandwidth to a LAN rather than to just one computer. Before customers can subscribe to cable modem service, however, their local cable company must have the necessary infrastructure.

Although the device that connects a subscriber's home computer to the cable infrastructure is called a cable modem, it is not a true modem. Rather it is a connectivity device containing network interfaces, similar to a hub or router.

Figure 7-11 A cable modem

Traditional cable TV supplies the infrastructure for downstream communication (the TV programming), but not for upstream communication. To provide Internet access through its network, the cable company must upgrade its existing equipment to support bidirectional, digital communications. For starters, the cable company's network wiring must be replaced with **hybrid fiber-coax (HFC)**, a very expensive fiber-optic link that can support high frequencies. The HFC connects the cable company's offices to a node location near the customer. Then, either fiber-optic or coaxial cable may connect the node to the customer's business or residence via a connection known as a **cable drop**. All cable drops for the cable subscribers in the same neighborhood connect to the local node. These nodes then connect to the cable company's central office, which is known as its **head-end**. At the head-end, the cable company can connect to the Internet through a variety of means (often via fiber-optic cable) or it can pick up digital satellite or microwave transmissions. The head-end can transmit data to as many as 1000 subscribers, in a one-to-many communication system. Figure 7-12 illustrates the infrastructure of a cable system.

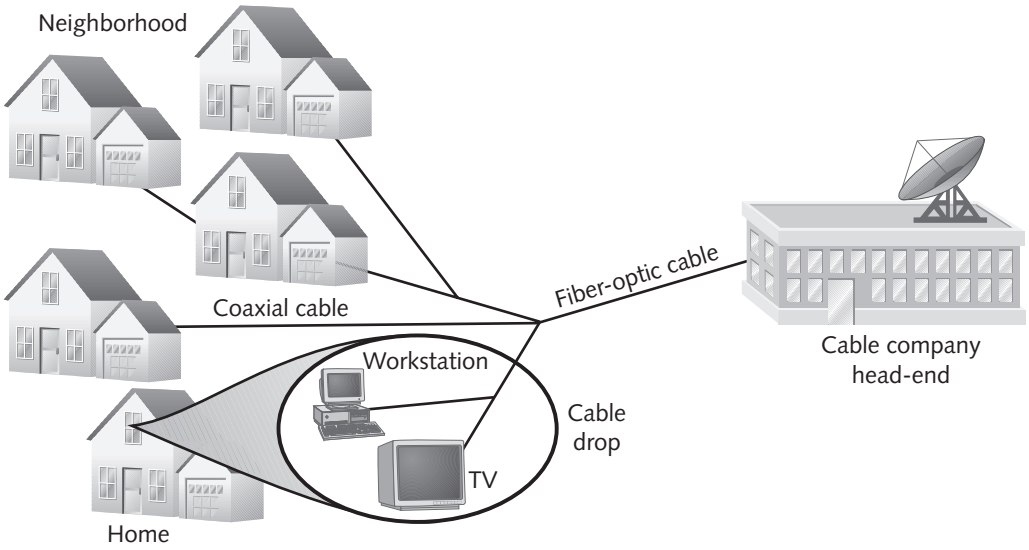

Figure 7-12 Cable infrastructure

One advantage of cable is that, like DSL, it provides a dedicated, or continuous, connection that does not require dialing up a service provider. On the other hand, cable technology requires many subscribers to share the same line, thus raising concerns about security and actual (versus theoretical) throughput. For example, if your cable company supplied you and five of your neighbors with cable access to the Internet, your neighbors could capture the data that you transmit to the Internet. Thus cable users must consider methods of securing their data, such as encryption. Moreover, the throughput of a cable line is fixed. As with any fixed resource, the more one claims, the less that is left for others. In other words, the greater the number of users sharing a single line, the less throughput available to each individual user.

Although cable competes with DSL for servicing consumers who demand higher bandwidth than that offered by PSTN or ISDN, it may not be able to keep up with the pace of DSL evolution. Instead, DSL may have the edge because its infrastructure (the PSTN) is already in place, while cable is not quite ubiquitous. Also, the prices of consumer DSL service have come down to nearly the same level as cable. Cable modems are less often used in businesses than DSL, partly because of security and bandwidth concerns that arise from its shared nature.

SONET (Synchronous Optical Network)

SONET (Synchronous Optical Network) can provide data transfer rates from 64 Kbps to 39.8 Gbps using the same TDM technique used by T-carriers. Bell Communications Research developed SONET technology in the 1980s to link different

phone systems around the world. SONET has since emerged as the best choice for linking WANs between North America, Europe, and Asia, because it can work directly with the different standards used in different countries. Internationally, SONET is known as **SDH (Synchronous Digital Hierarchy)**. SONET integrates well with T-carriers, making it a good choice for connecting WANs and LANs over long distances (even within the same country). In fact SONET is often used to aggregate multiple T1s or T3s. SONET is also used as the underlying technology for ATM transmission.

SONET depends on fiber-optic transmission media to achieve its extraordinary quality of service and throughput. Like T-carriers, it also uses multiplexers and terminal equipment to connect at the customer's end. A typical SONET network takes the form of a ring topology, similar to FDDI, in which one ring acts as the primary route for data and a second ring acts as a backup. If, for example, a backhoe operator severs one of the rings, SONET technology would automatically reroute traffic along the backup ring. This characteristic, known as **self-healing**, makes SONET very reliable. Companies can lease an entire SONET ring from their local or long-distance carrier or they can lease part of a SONET, a circuit that offers T1 throughput, to take advantage of SONET's reliability. Figure 7-13 illustrates a SONET ring and its dual-fiber connections.

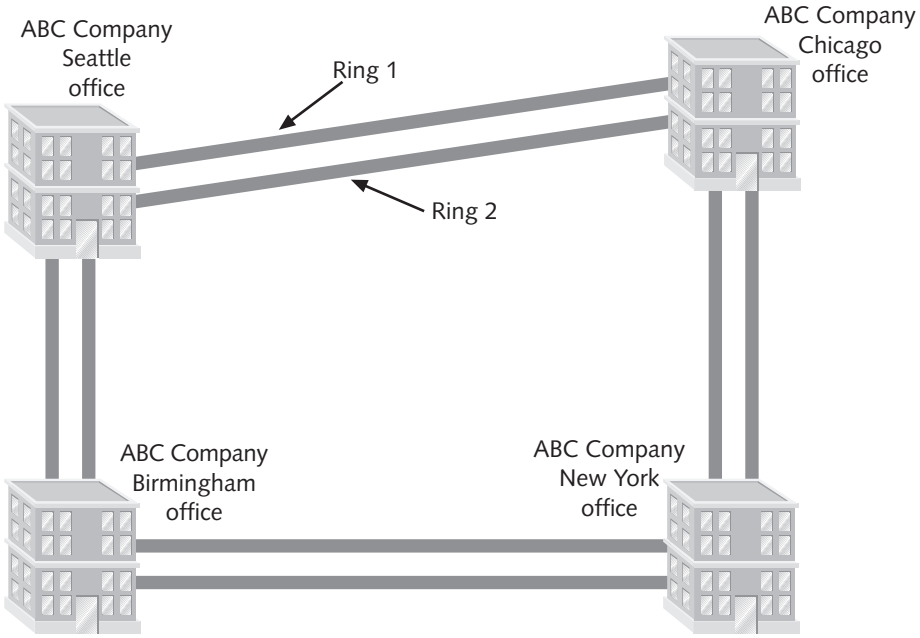

Figure 7-13 SONET technology on a long-distance WAN

The data rate of a particular SONET ring is indicated by its Optical Carrier (OC) level, a rating that is internationally recognized by networking professionals and standards organizations. OC levels in SONET are analogous to the digital signal levels of T1s. Table 7-3 lists the OC levels and their maximum throughput.

Table 7-3 SONET OC levels

OC Level	Throughput (Mbps)
OC1	51.84
OC3	155.52
OC12	622
OC24	1244
OC48	2480
OC96	4976
OC192	9953
OC768	39813

SONET technology is typically not implemented by small or medium-sized businesses, because of its high cost. It is more commonly used by large global companies, long-distance companies linking metropolitan areas and countries, or ISPs that want to guarantee fast, reliable access to the Internet. SONET is particularly suited to audio, video, and imaging data transmission. As you can imagine, given its reliance on fiber-optic cable and its redundancy requirements, SONET technology is very expensive to implement.

WAN Implementation

You need to weigh many factors when choosing a WAN for your organization. Among other things, you need to consider how well a new WAN will integrate with your existing LAN or WAN equipment, the transmission speed that is required by your users and applications, the kind of security you need, the geographical distance spanned by your WAN, the extent to which the WAN might grow over time and, of course, your budget. This section compares the WAN technologies mentioned previously on the basis of the most significant and predictable factors: speed, reliability, and security. Although cost is, of course, an important factor, it will vary dramatically depending on your circumstances. For cost estimates, you should contact an ISP or a local or long-distance service provider.

Speed

You have learned that WAN links offer a wide range of transmission speeds, from 56 Kbps for a PSTN dial-up connection to potentially 39.8 Gbps for a full-speed SONET connection. Table 7-4 summarizes the speeds offered by each technology discussed in this chapter. Bear in mind that each technology's transmission techniques (for example, switching for frame relay versus point-to-point for T1) will affect real throughput, so the maximum transmission speed is a theoretical limit. Actual transmission speeds will vary.

Table 7-4 A comparison of WAN technology transmission speeds

WAN Technology	Typical Media	Maximum Transmission Speed
Dial-up over PSTN	UTP or STP	56 Kbps
X.25	UTP/STP (DS1 or DS3)	64 Kbps or 2.048 Mbps
frame relay	UTP/STP (DS1 or DS3)	45 Mbps
BRI (ISDN)	UTP/STP (PSTN)	64–128 Kbps
PRI (ISDN)	UTP/STP (PSTN)	1.544 Mbps
T1	UTP/STP (PSTN), microwave, or fiber-optic cable	1.544 Mbps
Fractional T1	UTP/STP (PSTN), microwave, or fiber-optic cable	*n* times 64 Kbps (where *n* = number of channels leased)
T3	Microwave or fiber-optic cable	45 Mbps
DSL	UTP/STP (PSTN)	1.544 Mbps–52 Mbps (depends on the type)
Cable	Hybrid fiber-coaxial cable	36 Mbps downstream, 10 Mbps upstream
SONET	Fiber-optic cable	51, 155, 622, 1244, 2480, 4976, 9952, or 39813 Mbps (depending on the OC level)

Reliability

WAN technologies vary in their reliability. A WAN's reliability depends partly on the transmission medium it uses (for example, fiber-optic cable is more reliable than copper wire) and partly on its topology and transmission methods (for example, a fully meshed WAN provides better reliability than a partially meshed WAN, because more potential data paths are available should one link fail). WAN technologies can be roughly divided as follows:

- *Not very reliable, suited to individual or unimportant transmissions:* PSTN dial-up
- *Sufficiently reliable, suited for day-to-day transmissions:* ISDN, T1, fractional T1, T3, DSL, cable, X.25, and frame relay
- *Very reliable, suited to mission-critical applications:* SONET

Although PSTN lines are the least reliable of all WAN technologies, they are adequate for most telecommuting purposes. Their reliability depends on the quality of the local phone connection to a user's residence, which will vary from city to city and from neighborhood to neighborhood. Some connections may be entirely digital; others (particularly in rural areas) may be analog. Some may be subject to more noise than others are. The quality of PSTN dial-up lines also depends on the quality of a user's modem, which will undoubtedly vary from user to user.

For employees picking up e-mail and data files from a business's branch offices across the state, ISDN or T1 lines will usually suffice. Some applications, however, require the highest reliability. For example, if you were transmitting a videoconference of a United Nations

meeting in New York to diplomats in Switzerland, you would want to use a very reliable technology such as SONET.

Security

Wise network managers will inspect security at every juncture in their WAN. Although fiber-optic media are the most secure transmission media (as you learned in Chapter 4), it's important to keep in mind that security is affected by more than simply the type of transmission media used. Among other things, you should consider the following issues:

- WAN security depends in part on the encryption measures each carrier provides for its lines. When leasing T1s, frame relay circuits, or SONET rings, you should ask a number of providers how they secure information in transit. In addition, you should verify that secure connectivity devices, such as firewalls, are employed at both ends of the connection. (You will learn about firewalls in detail in Chapter 15.)
- Enforce password-based authorization for LAN and WAN access and teach users how to choose difficult-to-decrypt passwords.
- Take the time to develop, publish, and enforce a security policy for users in your organization.
- Maintain restricted access to network equipment rooms and data centers.

All of these factors contribute to the security of your network. In other words, the type of WAN you choose does not affect security as much as the security considerations that apply to all networks. Network security is discussed further in Chapter 15.

Virtual Private Networks (VPNs)

Virtual private networks (VPNs) are wide area networks logically defined over public transmission systems that serve an organization's users, but isolate that organization's traffic from other users of the same public lines. They provide a way of constructing a WAN from existing public transmission systems. For example, an organization can carve out a private WAN on the Internet to serve only its offices across the country, while keeping the data secure and isolated from other (public) traffic.

Because VPNs do not require leasing a full T1 circuit, for example, or paying for a frame relay system, they provide inexpensive solutions for creating long-distance WANs. VPNs employ specific protocols and security techniques to ensure that data can be interpreted only at the WAN's nodes. The security techniques used may be purely software-based or they may include hardware such as a firewall. You will learn more about VPN security techniques in Chapter 15.

The software required to establish VPNs is usually inexpensive, in some cases being included with other widely used software. For example, Windows 2000 Server comes with a remote access utility called RAS that allows you to create a simple VPN. For

Novell-based networks, you can use BorderManager, a NetWare add-on product, to construct VPNs. In addition, many other companies offer software that will work with either of these network operating systems to create VPNs. Figure 7-14 depicts one possible implementation of a VPN. The beauty of VPNs is that they are tailored to a customer's distance and bandwidth needs, so, of course, every one is different.

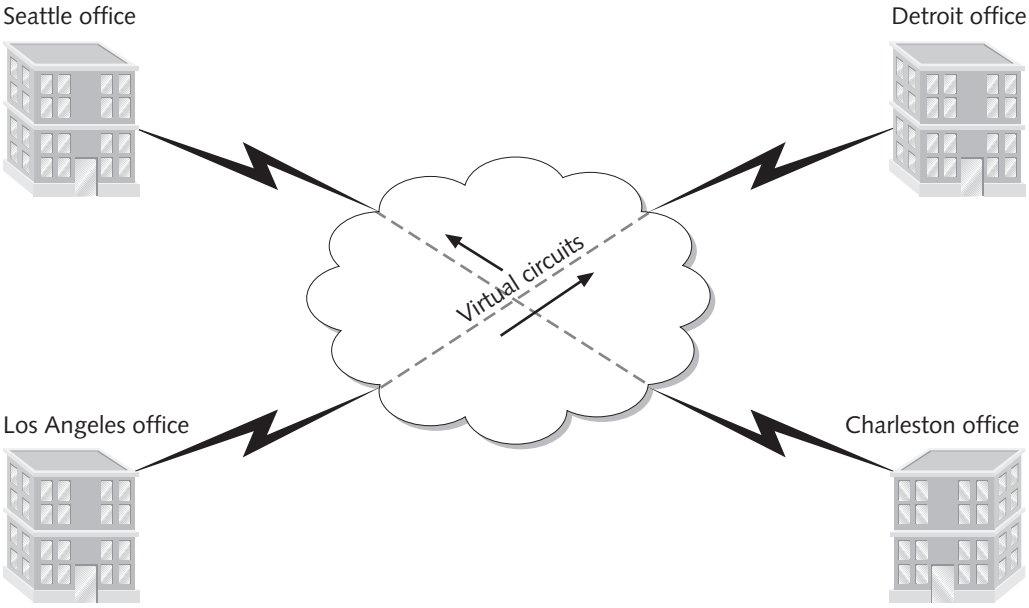

Figure 7-14 An example of a VPN

Do not confuse virtual private networks (VPNs) with the virtual LANs (VLANs) discussed in Chapter 6. VLANs are logically defined LANs created from an organization's existing LAN or WAN infrastructure, usually to serve a particular group of users.

Remote Connectivity

You have learned about almost every type of connection available for long-distance networking, but you may not know how the average user connects to a WAN. In a large organization with an enterprise-wide network, using a WAN is no different from using a LAN. You might log onto your company's network in Dallas, open Windows Explorer, and choose to view a PowerPoint presentation on a server in Phoenix. Your computer doesn't care about the location of the presentation file, because the WAN link makes it appear to be part of one big network (assuming that the network manager has done his or her job!). If you are at home or on the road, however, connecting to a WAN or LAN is somewhat different.

As a remote user, you must connect to a LAN via **remote access**, which can be accomplished in one of three ways: use a modem to dial directly into the LAN, use a modem to dial directly to a workstation, or use an Internet connection with a Web interface. Each of these methods offers different advantages and disadvantages, as described in the following material. Bear in mind that the true limiting factor in a remote connection is typically the speed of the modem, PSTN, or other access method that you're using.

- *Direct dial to the LAN*—The client uses dial-in software supplied with its operating system to connect to a remote access server on the LAN. As you learned in Chapter 1, a remote access server (also called a dial-in server) is a combination of software and hardware that provides a central access point for multiple users to dial into a LAN or WAN. The LAN treats the direct-dial remote client like any other client on the LAN; that is, the remote user can perform the same functions he or she could perform while in the office. The computer dialing into the LAN becomes a **remote node** on the network. Although this remote access method is the most complex to configure, especially on the server side, it can provide the best security. Also, the transmission speed of a direct-dial connection does not suffer when the Internet becomes congested. With the proper server hardware and software, this kind of connection can offer multiple users simultaneous remote access to the LAN.
- *Direct dial to a workstation*—The remote client uses dial-in software supplied with its operating system to connect to a workstation that is directly attached to the LAN. Software (such as Symantec's pcAnywhere) running on both the remote user's computer and the LAN computer allows the remote user to "take over" the LAN workstation, a solution known as **remote control**. Remote control is not as difficult to configure and confers the same security and throughput benefits as directly dialing into a remote access server. In addition, this method provides the best performance for processing-intensive applications such as databases, because the data processing can occur on the LAN-attached workstation without having to traverse the slower modem connection to the remote workstation. One disadvantage to this solution is that it allows only one connection to the LAN at any given time.
- *Internet/Web interface*—Through a browser such as Netscape Communicator or Microsoft's Internet Explorer, a user at home or on the road connects to a LAN whose files are made visible to the Web through Web server software. This method requires some setup steps on both the client and the server, but it is not usually as complex as a direct-dial configuration. Its security and throughput cannot be controlled as thoroughly as those of the direct-dial solutions, however, because the remote user's connection is not dedicated. Nevertheless, a Web interface is very simple to use and widely available. Also, a nearly unlimited number of remote users can simultaneously access the LAN resources using this method.

Remote connectivity can be established between almost any combination of workstation and operating system, given the appropriate software and hardware configuration. A popular method for gaining remote access to LANs is by using Citrix System, Inc.'s **ICA (Independent Computing Architecture) client** to connect with a remote access server. Once installed on a remote user's workstation, the ICA client enables the workstation to communicate with the LAN from anywhere over any type of connection, public or private. Because the ICA client exchanges only keystrokes, mouse clicks, and screen updates with the server, this type of remote access is particularly well suited to slower connections, such as dial-up PSTN connections. Citrix's ICA client can work with virtually any operating system or application. Its ease of use and broad compatibility has made the ICA client one of the most popular methods for supplying widespread remote access across an organization. In order to function properly, the ICA requires Citrix's remote access software running on the access server. Potential drawbacks to this method include cost of Citrix's products and the complex nature of its server software configuration.

Perhaps the simplest dial-in server is the **Remote Access Service** (**RAS**, pronounced "razz"), which comes with Windows 2000 Server. Because it is a good example of a remote access server, you should investigate RAS when you work with Windows 2000 servers. Knowing RAS will help you understand more complex access server technologies.

In addition to Microsoft's remote access methods, networking hardware manufacturers such as Bay Networks, Cisco Systems, and 3Com market their own remote access technologies. In addition, a number of specialized software companies provide programs that run on Windows 2000, NetWare, or UNIX servers. The method you choose will depend on your requirements for security, throughput, number of connections, and cost, and the technical expertise of your users and support staff. If you enable remote access for your network, you will need to be familiar with the process of configuring clients for connection and be able to support those clients. The next section describes how to configure a dial-up networking client.

Dial-Up Networking

Dial-up networking refers to the process of dialing into a LAN's (private) access server or to an ISP's (public) access server to log onto a network. Most telecommuters use some form of dial-up networking to connect to their LAN. This section describes how to configure a workstation to dial into a remote access server. For discussion purposes, the example of a Windows 2000 Professional client logging onto a private access server is used. Later, in the projects at the end of this chapter, you will have the opportunity to create a dial-up networking connection that enables you to log onto an ISP's access server.

First make sure that your modem is installed and working properly. To create a new dial-up connection:

1. Click **Start**, point to **Settings**, and then click **Network and Dial-up Connections**. The Network and Dial-up Connections window appears.

2. Double-click the **Make New Connection** icon. The Network Connection Wizard opens.
3. If you have not previously configured a dial-up connection on your computer, you will be asked to provide your area code in the Location Information dialog, and then click **OK**. Then you will be asked to provide your location in the Phone and Modem Options dialog and click **OK**. Click **Next** to continue.
4. You are prompted to identify the type of dial-up connection you want to create, as shown in Figure 7-15. For this exercise, select **Dial-up to private network**, then click **Next** to continue.

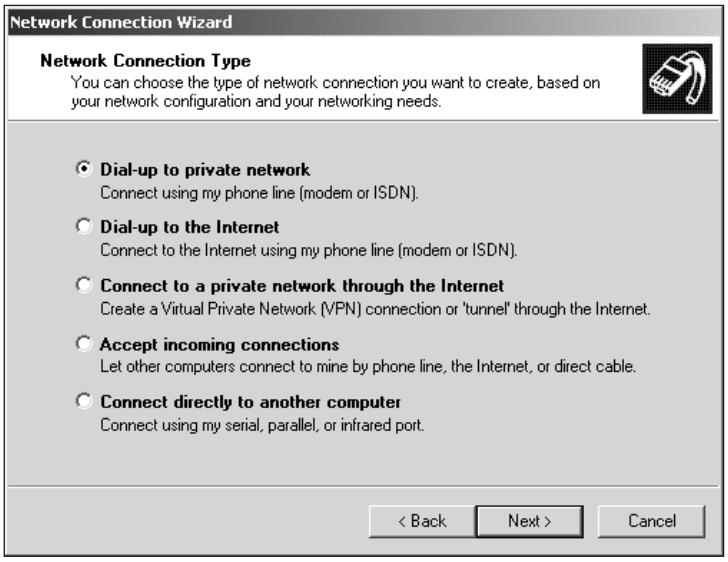

Figure 7-15 Choosing a network connection type

5. At the next screen you are prompted to enter the number of the RAS server. Type the server's dial-up number and click **Next** to continue.
6. You are prompted to select the availability of the connection—whether you want the connection available to all users or only to the user under whose ID you are currently logged in. For this exercise, keep the default selection of **For all users**, then click **Next** to continue.
7. You are asked to name the connection. Type a word or phrase that will help you identify this connection when it appears as an icon in your Network and Dial-up Connections window.
8. Click **Finish** to complete the task of creating a new dial-up connection.

After creating a new Dial-up Networking profile, you may need to configure its connectivity options. Unless you configure it precisely according to the server's parameters, your connection will not work properly. In some cases, if you enter incomplete or incorrect information, you may be able to establish a session between your client and the server, but be unable to send or receive data. If you are dialing into an ISP's server, the ISP will provide the information used for this configuration.

The following steps provide an example of how to configure a dial-up connection:

1. In the Network and Dial-up Connections window, right-click the connection you want to configure. A shortcut menu opens.
2. Click **Properties**. A Properties window (whose title begins with the name of your profile) opens.
3. Click the **Networking** tab to display the network properties, including the type of dial-up server and network components that are available to this connection. The Type of dial-up server option provides a choice between PPP or SLIP connections. (PPP and SLIP connections are discussed in the next section.) Your RAS server will probably use PPP, which is selected as the default. However, you should check to make sure the proper type of server is selected. If you select the wrong type, you will not be able to connect to the ISP's server.
4. In the list of components used by this connection, make sure that the "Client for Microsoft Networks" and the "Internet Protocol (TCP/IP)" check boxes are checked. If other components (for example, the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol) are selected, deselect them.
5. Double-click the **Internet Protocol (TCP/IP)** component to view its properties. The default options of "Obtain an IP address automatically" and "Obtain DNS server address automatically" are probably the options your server will require. However, if your RAS server does not assign IP addresses automatically, you will need to obtain an IP address and DNS server address from your network administrator and enter them here.
6. Click **OK** to close the Internet Protocol (TCP/IP) Properties dialog box.

If you have both a modem and a NIC on your PC, changing the TCP/IP properties for the dial-up connection will not affect the TCP/IP properties you have set for your NIC. In Network properties, you will see that TCP/IP is bound to both your NIC and your Dial-up Adapter and that the properties differ for each TCP/IP binding.

7. Click the **Security** tab. Here you can choose the level of security you want for your connection. The default level is to accept an unsecured password, which means that the password you use to log onto the RAS server does not need to meet strict password guidelines (for example, a length of at least eight characters). For this exercise, click the down arrow next to this default option and choose **Require secured password** from the drop-down list.

8. Notice that the options below the drop-down box become available. Select the **Automatically use my Windows logon name and password (and domain if any)** option.
9. Click the **Options** tab to view and modify some general properties of this dial-up connection.
10. Here you can change the nature of how your connection is dialed, including how many times the computer will redial if it fails to connect the first time. Choose the **Redial if line is dropped** option.
11. Click **OK** to close the Dial-up Connection properties dialog box and save your changes.
12. Test your connection to the remote server.

Now that you have become familiar with remote connectivity methods and know how to create and configure a dial-up networking profile, you will learn about the two most common dial-up networking protocols, PPP and SLIP. In order to qualify for Net+ certification, you should understand how to assign these protocols to a dial-in connection; you should also understand the differences between the two protocols.

Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP)

Serial Line Internet Protocol (SLIP) and **Point-to-Point Protocol (PPP)** are two communications protocols that enable a workstation to connect to a server using a serial connection (in the case of dial-up networking, *serial connection* refers to a modem). Such protocols are necessary to transport Network layer traffic over serial interfaces, which belong to the Data Link layer of the OSI Model. Both SLIP and PPP encapsulate higher-layer networking protocols in their lower-layer data frames. SLIP is a version of the protocol that can carry only IP packets, however, and PPP can carry many different types of Network layer packets, such as IPX or AppleTalk. Another difference between SLIP and PPP is that SLIP supports only asynchronous data transmission and PPP supports both asynchronous and synchronous transmission.

Asynchronous refers to a communications method in which data being transmitted and received by nodes do not have to conform to any predetermined schemes that specify when they can transmit data. In asynchronous communications, a node can transmit at any time, and the destination node must accept the transmission as it comes. To ensure that the receiving node knows when it has received a complete frame, asynchronous communications provide start and stop bits for each character transmitted. When the receiving node recognizes a start bit, it begins to accept a new character. When it receives the stop bit for that character, it ceases to look for the end of that character's transmission. Asynchronous data transmission therefore occurs in random stops and starts.

Conversely, **synchronous** refers to a communications method in which data being transmitted and received by nodes must conform to a timing scheme. A clock maintains time for all nodes on a network. A receiving node in synchronous communications recognizes

that it should be receiving data by looking at the time on the clock. In synchronous communications, start and stop bits are not necessary, because the clocking indicates where transmission should begin and where it should end. As an analogy, imagine a marathon with 1000 participants, in which each runner starts the race precisely five minutes after the previous runner started. The race's official timekeeper keeps track of when each runner begins, so that when a runner arrives at the finish line, his or her total time can be calculated. Runner B, who starts ten minutes after Runner A, will not be expected to arrive at the finish line at the same time as Runner A. In this analogy, the race official is like the clocking mechanism in synchronous communications.

PPP is the more popular communications protocol for dial-up connections to the Internet, primarily because it does not require as much configuration on the client as SLIP does. When using SLIP, you typically have to specify the IP addresses for both your client and for your server in your dial-up networking profile. PPP, on the other hand, can automatically obtain this information as it connects to the server. Because it is more difficult to configure, SLIP is rarely used.

Chapter Summary

- WANs are distinguished from LANs by the fact that WANs traverse a wider geographical area. They usually employ point-to-point communications rather than point-to-many communications (where LAN hubs or switches connect multiple segments or workstations). WANs also provide better and faster transmission than LANs.
- WAN transmission methods differ in terms of their speed, reliability, cost, distance covered, and security. For every business need, only one or a handful of appropriate WAN transmission methods may exist. Several WAN technologies may be used together on the same network.
- One WAN transmission method, PSTN (Public Switched Telephone Network), relies on the network of telephone lines that typically services homes. The PSTN was originally composed of analog lines but now uses digital transmission over fiber-optic and copper twisted-pair cable, microwave, and satellite connections. PSTN is usually adequate for at-home dial-up LAN or Internet users.
- A remote user can use the PSTN to access a remote server via a dial-up connection. In a dial-up connection, the user's modem converts the computer's digital pulses into analog signals. These signals travel through PSTN to the receiving computer's modem, which then converts the analog signals back into digital pulses. Unlike other types of WAN connections, dial-up connections provide a fixed period of access to the network.
- X.25 is an analog, packet-switched technology optimized for long-distance data transmission and standardized by the ITU in the mid-1970s. It can support 2-Mbps throughput. X.25 was originally developed and used for communications between mainframe computers and remote terminals. Though rare in North America, it remains a WAN standard around the world.

- Frame relay also relies on packet switching. Because it is digital, and because it does not analyze frames, but simply relays them from node to node, frame relay supports higher bandwidth than X.25, offering a maximum of 45-Mbps throughput.
- Both X.25 and frame relay are configured as permanent virtual circuits (PVCs). PVCs are point-to-point connections over which data may follow any number of different paths. When you lease an X.25 or frame relay circuit from your local carrier, your contract reflects the endpoints you specify and the amount of bandwidth required between those endpoints.
- Another WAN transmission method, ISDN (Integrated Services Digital Network), is an international standard established by the ITU for transmitting data over digital lines. ISDN uses the telephone carrier's lines and dial-up connections, like PSTN. It differs from PSTN in that it travels exclusively over digital lines and switches.
- ISDN lines may carry voice and data signals simultaneously, but require an ISDN phone to carry voice traffic and an ISDN router and ISDN terminal adapter to carry data. ISDN lines circumvent the need to pay for separate phone lines to support faxes, modems, and voice calls at one location.
- Two types of ISDN connections are commonly used by consumers in North America: Basic Rate Interface (BRI) and Primary Rate Interface (PRI).
- BRI uses two 64-Kbps circuit-switched bearer channels (or B channels) to transmit and receive data or voice. These two channels carry the traffic from point to point. An additional 16-Kbps channel called a D channel, for "data" channel, carries information about the call, such as session initiation and termination signals, caller identity, call forwarding, and conference calling signals.
- B channels in ISDN lines are treated as separate connections by the network and can carry voice and data or two data streams simultaneously and separate from each other. A process called bonding can combine the throughput of the B channels into a larger effective throughput.
- PRI uses 23 B channels and one 64-Kbps D channel. Individual subscribers rarely use PRI, preferring BRI instead, but PRI may be used by business and other organizations needing more throughput. The maximum potential throughput for a PRI connection is 1.544 Mbps, the same as that for a T1 circuit.
- Another WAN transmission method is digital subscriber line (DSL). DSL uses advanced data modulation techniques to achieve extraordinary throughput over regular phone lines. Data modulation uses one signal to alter the frequency, phase, or amplitude of another signal. In the case of DSL, multiple high-frequency carrier signals are modulated by modems' data signals, enabling DSL connections to support high throughput over copper wire.
- DSL comes in seven different varieties, each of which is either asymmetrical or symmetrical. In asymmetrical transmission, more data can be sent in one direction than in the other direction. In symmetrical transmission, equal amounts of data can be sent in either direction. The most popular form of DSL is ADSL.

- DSL technology creates a dedicated circuit. At the consumer end, a DSL modem connects computers and telephones to the DSL line. At the carrier end, a DSL access multiplexer (DSLAM) aggregates multiple incoming DSL lines before connecting them to the Internet or to larger carriers.
- Cable is another option for high bandwidth local loop WAN transmission. Cable relies on the cable wiring used for TV signals. Such wiring could realistically transmit approximately 3 to 10 Mbps downstream and 2 Mbps upstream. The asymmetry of cable technology makes it a logical choice for users who want to surf the Web or download data from a network.
- Cable connections require that the customer use a special cable modem to transmit and receive signals over cable wiring. In addition, most cable companies will have to replace part of their coaxial cable plant with fiber-optic cable to support bidirectional, digital communications.
- Like DSL, cable provides a dedicated, or continuous, connection that does not require dialing up a service provider.
- T-carrier technology uses time division multiplexing (TDM) to divide a single channel into multiple channels for carrying voice, data, video, or other signals. Devices at the sending end arrange the data streams (multiplex), then devices at the receiving end filter them back into separate signals (demultiplex).
- A number of T-carrier varieties are currently available. The most common T-carrier implementations are T1 and, for higher bandwidth needs, T3. A T1 circuit can carry the equivalent of 24 voice channels, giving a maximum data throughput of 1.544 Mbps. A T3 can carry the equivalent of 672 voice channels, giving a maximum data throughput of 44.736 Mbps.
- The signal level of a T-carrier refers to its Physical layer electrical signaling characteristics, as defined by ANSI standards in the early 1980s. DS0 is the equivalent of one data or voice channel. All other signal levels are multiples of DS0.
- A fractional T1 lease allows organizations to use only some channels on a T1 line and pay for only those channels actually used. Thus fractional T1 bandwidth can be leased in multiples of 64 Kbps. A fractional T1 is suited to businesses that expect their traffic to grow and that can't currently justify leasing a full T1.
- T1 technology can use unshielded or shielded twisted-pair copper wiring. Because the digital signals require a cleaner connection, shielded twisted-pair is considered preferable. Twisted-pair wiring cannot adequately carry the high throughput of multiple T1s or T3 transmissions. For multiple T1s, coaxial cable may be used or either of the T3 transmission media—either microwave or fiber-optic cabling.
- The CSU/DSU is the connection point for a T1 line at the customer's site. The CSU provides termination for the digital signal and ensures connection integrity through error correction and line monitoring. The DSU converts the digital signal used by bridges, routers, and multiplexers into the digital signal carried via cabling.

- The devices that connect to the multiplexer are collectively known as terminal equipment. On a typical T1-connected data network, this equipment consists of bridges and/or routers. A bridge or router would typically integrate two types of networks: the incoming T1 (Internet) and an Ethernet or Token Ring LAN at the customer's site.
- SONET can provide data transfer rates from 64 Kbps to 39.8 Gbps using the same TDM technique employed by T-carriers. It is the best choice for linking WANs between North America, Europe, and Asia, because it can link directly with the different standards used in different countries.
- Internationally, SONET is known as SDH (Synchronous Digital Hierarchy). SONET integrates well with T-carriers, ISDN, and ATM technology.
- SONET depends on fiber-optic transmission media and uses multiplexers and terminal equipment to connect at the customer's end. A typical SONET network takes the form of a ring topology. If one ring breaks, SONET technology automatically reroutes traffic along a backup ring. This characteristic, known as self-healing, makes SONET very reliable.
- SONET technology is typically implemented by large global companies, long-distance companies linking metropolitan areas and countries, or ISPs that want to guarantee fast, reliable access to the Internet. SONET is particularly suited to audio, video, and imaging data transmissions but is very expensive.
- When implementing a new WAN installation or upgrade, you should consider the following factors: the WAN's ability to integrate with your existing LAN or WAN equipment, the kind of transmission speed required by your users and applications, the kind of security needed, the geographical distance the WAN must span, the extent to which the WAN might grow over time, and, of course, the expense.
- Virtual private networks (VPNs) represent one way to construct a WAN from existing public transmission systems. An organization can carve out a private WAN on the Internet (or over leased lines) to serve only its offices, while keeping the data secure and isolated from other (public) traffic.
- As a remote user, you can connect to a LAN in one of three ways: direct dial to the LAN, direct dial to a workstation, or an Internet connection with a Web interface. Each method has different advantages and disadvantages pertaining to its throughput, security, complexity, and number of simultaneous users allowed.
- Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) are communications protocols that enable a workstation to connect to a server using a serial connection (in the case of dial-up networking, "serial connection" refers to a modem). Such protocols are necessary to transport Network layer traffic over serial interfaces, which belong to the Data Link layer of the OSI Model. Because it is easier to configure and supports more than one type of Network layer protocol, PPP is preferred over SLIP.

KEY TERMS

asymmetrical — The characteristic of a transmission technology that affords greater bandwidth in one direction (either from the customer to the carrier, or vice versa) than in the other direction.

asymmetrical DSL — A variation of DSL that offers more throughput when data travels downstream—downloading from a local carrier's POP to the customer—than when it travels upstream—uploading from the customer to the local carrier's POP.

asynchronous — A transmission method in which data being transmitted and received by nodes do not have to conform to any timing scheme. In asynchronous communications, a node can transmit at any time and the destination node must accept the transmission as it comes.

B channel — In ISDN, the "bearer" channel, so named because it bears traffic from point to point.

bonding — The process of combining more than one bearer channel of an ISDN line to increase throughput. For example, BRI's two 64-Kbps B channels are bonded to create an effective throughput of 128 Kbps.

BRI (Basic Rate Interface) — A variety of ISDN that uses two 64-Kbps bearer channels and one 16-Kbps data channel, as summarized by the following notation: 2B + D. BRI is the most common form of ISDN employed by home users.

broadband — A group of network connection types or transmission technologies that are generally capable of exceeding 1.544 Mbps throughput. Examples of broadband include DSL and SONET.

cable drop — Fiber-optic or coaxial cable that connects a neighborhood cable node to a customer's house.

cable modem — A device that modulates and demodulates signals for transmission and reception via cable wiring.

CIR (committed information rate) — The guaranteed minimum amount of bandwidth selected when leasing a frame relay circuit. Frame relay costs are partially based on CIR.

CSU (channel service unit) — A device used with T-carrier technology that provides termination for the digital signal and ensures connection integrity through error correction and line monitoring.

CSU/DSU — A combination of a CSU (channel service unit) and a DSU (data service unit) that serves as the connection point for a T1 line at the customer's site.

D channel — In ISDN, the "data" channel used to carry information about the call, such as session initiation and termination signals, caller identity, call forwarding, and conference calling signals.

dedicated — A continuously available link or service that is leased through another carrier. Examples of dedicated lines include ADSL, T1, and T3.

dial-up — A type of connection that uses modems at the transmitting and receiving ends and PSTN or other lines to access a network.

dial-up networking — The process of dialing into a LAN's access server or into an ISP. Dial-up Networking is also the name of the utility that Microsoft provides with its operating systems to achieve this type of connectivity.

downstream — A term used to describe data traffic that flows from a local carrier's POP to the customer. In asymmetrical communications, downstream throughput is usually much higher than upstream throughput. In symmetrical communications, downstream and upstream throughputs are equal.

DS0 (digital signal, level 0) — The equivalent of one data or voice channel in T-carrier technology, as defined by ANSI physical layer standards. All other signal levels are multiples of DS0.

DSL (digital subscriber line) — A dedicated remote connectivity or WAN technology that uses advanced data modulation techniques to achieve extraordinary throughput over regular phone lines. DSL currently comes in seven different varieties, the most common of which is Asymmetric DSL (ADSL).

DSL access multiplexer (DSLAM) — A connectivity device located at a carrier's office that aggregates multiple DSL subscriber lines and connects them to a larger carrier or to the Internet backbone.

DSL modem — A device that demodulates an incoming DSL signal, extracting the information and passing it on to the data equipment (such as telephones and computers) and modulates an outgoing DSL signal.

DSU (data service unit) — A device used in T-carrier technology that converts the digital signal used by bridges, routers, and multiplexers into the digital signal used on cabling. Typically, a DSU is combined with a CSU in a single box, a CSU/DSU.

Federal Communications Commission (FCC) — The regulatory agency that sets standards and policy for telecommunications transmission and equipment in the United States.

fractional T1 — An arrangement that allows organizations to use only some channels on a T1 line and pay for only the channels actually used.

frame relay — An updated, digital version of X.25 that relies on packet switching. Because it is digital, frame relay supports higher bandwidth than X.25, offering a maximum of 45-Mbps throughput. It provides the basis for much of the world's Internet connections. On network diagrams, the frame relay system is often depicted as a cloud.

head-end — A cable company's central office, which connects cable wiring to many nodes before it reaches customers' sites.

hybrid fiber-coax (HFC) — A link that consists of fiber cable connecting the cable company's offices to a node location near the customer and coaxial cable connecting the node to the customer's house. HFC upgrades to existing cable wiring are required before current TV cable systems can serve as WAN links.

ICA (Independent Computing Architecture) client — A remote access client developed by Citrix Systems, Inc. that enables remote users to use virtually any LAN application over any type of connection, public or private. The ICA client is especially well suited to slower connections, as it exchanges only keystrokes, mouse clicks, and screen updates with the server. The ICA client requires that Citrix's server software run on the access server.

ISDN (Integrated Services Digital Network) — An international standard, established by the ITU, for transmitting data over digital lines. Like PSTN, ISDN uses the telephone carrier's lines and dial-up connections, but it differs from PSTN in that it exclusively uses digital lines and switches.

leased lines — Permanent dedicated connections established through a public telecommunications carrier and billed to customers on a monthly basis.

local loop — The part of a phone system that connects a customer site with a public carrier's POP. Some WAN transmission methods, such as ISDN, are suitable for only the local loop portion of the network link.

multiplexer — In the context of T-carrier technology, a device that provides the means of combining multiple voice and/or data channels on one line. Multiplexers can take input from a variety of terminal equipment, such as bridges, routers, or telephone exchange devices, for use with voice traffic.

Network Termination 1 (NT1) — A device used on ISDN networks that connects the incoming twisted-pair wiring with the customer's ISDN terminal equipment.

Network Termination 2 (NT2) — An additional connection device required on PRI to handle the multiple ISDN lines between the customer's network termination connection and the local phone company's wires.

plain old telephone service (POTS) — See *PSTN*.

point of presence (POP) — The place where the two telephone systems meet—either a long-distance carrier with a local telephone company or a local carrier with an ISP's facility.

Point-to-Point Protocol (PPP) — A communications protocol that enables a workstation to connect to a server using a serial connection. PPP can support multiple Network layer protocols, can use both asynchronous and synchronous communications, and does not require much (if any) configuration on the client workstation.

PRI (Primary Rate Interface) — A type of ISDN that uses 23 bearer channels and one 64-Kbps data channel as represented by the following notation: 23B + D. PRI is less commonly used by individual subscribers than BRI, but it may be used by businesses and other organizations needing more throughput.

PSTN (Public Switched Telephone Network) — The network of typical telephone lines that has been evolving for 100 years and still services most homes.

PVC (permanent virtual circuit) — A point-to-point connection over which data may follow any number of different paths, as opposed to a dedicated line that follows a predefined path. X.25, frame relay, and some forms of ATM use PVCs.

remote access — A method for connecting and logging onto a LAN from a workstation that is remote, or not physically connected, to the LAN. Remote access can be accomplished one of three ways: by using a modem to dial directly into the LAN; by using a modem to dial directly to a workstation; or by using an Internet connection with a Web interface. Remote access may complete a connection via public or private lines.

remote access server — A combination of software and hardware that provides a central access point for multiple users to dial into a LAN or WAN.

Remote Access Service (RAS) — One of the simplest dial-in servers. This software is included with Windows 2000 Server. Note that RAS is pronounced *"razz"*.

remote control — A remote access method in which the remote user dials into a workstation that is directly attached to a LAN. Software running on both the remote user's computer and the LAN computer allows the remote user to "take over" the LAN workstation.

remote node — A client that has dialed directly into a LAN's remote access server. The LAN treats a remote node like any other client on the LAN, allowing the remote user to perform the same functions he or she could perform while in the office.

SDH (Synchronous Digital Hierarchy) — The international equivalent of SONET.

self-healing — A characteristic of dual-ring topologies that allows them to automatically reroute traffic along the backup ring if the primary ring becomes severed.

Serial Line Internet Protocol (SLIP) — A communications protocol that enables a workstation to connect to a server using a serial connection. SLIP can support only asynchronous communications and IP traffic, and requires some configuration on the client workstation.

signal level — An ANSI standard for T-carrier technology that refers to its Physical layer electrical signaling characteristics. DS0 is the equivalent of one data or voice channel. All other signal levels are multiples of DS0.

SONET (Synchronous Optical Network) — A WAN technology that provides data transfer rates ranging from 64 Kbps to 39.8 Gbps, using the same time division multiplexing technique used by T-carriers. SONET is the best choice for linking WANs between North America, Europe, and Asia, because it can link directly using the different standards used in different countries.

SVC (switched virtual circuit) — Logical, point-to-point connections that rely on switches to determine the optimal path between sender and receiver. ATM technology uses SVCs.

symmetrical — A characteristic of transmission technology that provides equal throughput for data traveling both upstream and downstream and is suited to users who both upload and download significant amounts of data.

symmetrical DSL — A variation of DSL that provides equal throughput both upstream and downstream between the customer and the carrier.

synchronous — A transmission method in which data being transmitted and received by nodes must conform to a timing scheme.

T1 — A T-carrier technology that provides 1.544-Mbps throughput and 24 channels for voice, data, video, or audio signals. T1s may use shielded or unshielded twisted-pair, coaxial cable, fiber-optic, or microwave links. Businesses commonly use T1s to connect to their ISP, and phone companies typically use at least one T1 to connect their central offices.

T3 — A T-carrier technology that can carry the equivalent of 672 channels for voice, data, video, or audio, with a maximum data throughput of 44.736 Mbps (typically rounded up to 45 Mbps for purposes of discussion). T3s require either fiber-optic or microwave transmission media.

T-carriers — The term for any kind of leased line that follows the standards for T1s, fractional T1s, T1Cs, T2s, T3s, or T4s.

terminal adapter (TA) — Devices used to convert digital signals into analog signals for use with ISDN phones and other analog devices. Terminal adapters are sometimes called ISDN modems.

terminal equipment (TE) — Devices that connect computers to the ISDN line. Terminal equipment may include standalone devices or cards (similar to the network adapters used on Ethernet and Token Ring networks) or ISDN routers.

upstream — A term used to describe data traffic that flows from a customer's site to the local carrier's POP. In symmetrical communications, upstream throughput is usually much lower than downstream throughput. In symmetrical communications, upstream and downstream throughputs are equal.

virtual private network (VPN) — A logically constructed WAN that uses existing public transmission systems. VPNs can be created through the use of software or combined software and hardware solutions. This type of network allows an organization to carve out a private WAN on the Internet (or, less commonly over leased lines) that serves only its offices, while keeping the data secure and isolated from other (public) traffic.

WAN link — The line that connects one location on a WAN with another location.

X.25 — An analog packet switched WAN technology optimized for long-distance data transmission and standardized by the ITU in the mid-1970s. X.25 can support 2-Mbps throughput. It was originally developed and used for communications between mainframe computers and remote terminals.

xDSL — Term used to refer to all varieties of DSL.

Review Questions

1. Name three networking scenarios that would require a WAN.
2. What kind of public lines do most telecommuters use for dial-up connections?
   a. DSL
   b. cable
   c. PSTN
   d. T1s
   e. SONET
3. What is the maximum throughput of a BRI ISDN line?
   a. 56 Kbps
   b. 128 Kbps
   c. 256 Kbps
   d. 56 Mbps
   e. 128 Mbps

4. What is the purpose of ISDN's D channel?
   a. to carry call session information
   b. to carry error-checking information
   c. to enable symmetrical transmission
   d. to enable time division multiplexing
   e. to carry the data "payload"
5. Which of the following WAN technologies is represented in network diagrams by a cloud?
   a. frame relay
   b. ISDN
   c. DSL
   d. cable
   e. T-carrier
6. Which of the following WAN links is the most reliable?
   a. frame relay
   b. DSL
   c. T1
   d. T3
   e. SONET
7. Which of the following customers would symmetrical DSL best suit?
   a. a home office user who researches technology on the Web
   b. a convention center that provides multiple businesses with videoconferencing facilities
   c. a car manufacturer that obtains specifications from its quality control team across town
   d. a radiology clinic that uploads and downloads real-time images to and from a hospital across town
   e. a home user who watches movies on the Web
8. What technique enables DSL to achieve high bandwidth over PSTN lines?
   a. full duplexing
   b. message switching
   c. packet switching
   d. data modulation
   e. framing

9. A home user of DSL is likely to connect to his external DSL modem through either of what two methods?
   a. IR port
   b. Parallel port
   c. Ethernet NIC
   d. USB port
   e. AUI port
10. DS1 is equivalent to T1 throughout the world. True or False?
11. Which two of the following are symmetrical versions of DSL?
    a. ADSL
    b. G.Lite
    c. HDSL
    d. SDSL
    e. VDSL
12. What technique does T1 technology use to transmit multiple signals over a single telephone line?
    a. wave division multiplexing
    b. time division multiplexing
    c. amplitude modulation
    d. frequency modulation
    e. phase modulation
13. One T3 is equivalent to how many T1s?
    a. 3
    b. 9
    c. 18
    d. 28
    e. 42
14. How many 64-Kbps channels does a single T1 circuit carry?
    a. 4
    b. 12
    c. 16
    d. 24
    e. 32
15. Why are SONET networks considered "self-healing"?

16. Which of the following is a drawback of cable modem technology, compared to DSL?
    a. Its standards are less developed.
    b. Its installation is more difficult.
    c. Multiple subscribers must share a fixed amount of bandwidth.
    d. It does not interface easily with Ethernet LANs.
    e. It is an asymmetrical technology, while DSL is symmetrical.
17. What is the maximum throughput supported by X.25 technology?
    a. 24 Kbps
    b. 128 Kbps
    c. 384 Kbps
    d. 1.455 Mbps
    e. 2.048 Mbps
18. What do frame relay and ATM connections have in common?
    a. Both rely on the Internet.
    b. Both utilize existing PSTN lines.
    c. Both rely on virtual circuits.
    d. Both are affordable technologies for small businesses.
    e. Both are capable of over 1-Gbps throughput.
19. Which of the following may limit a DSL connection's capacity?
    a. the number of different customers who share the connection
    b. the distance from the customer to the carrier's POP
    c. the existence of more than one copper-wire phone line at the customer's location
    d. the distance from the carrier's POP to the ISP
    e. the lack of a splitter between the DSL modem and the carrier's POP
20. What does "CSU/DSU" stand for?
    a. channel service unit/data service unit
    b. communications server unit/digital server unit
    c. communications serial unit/data serial unit
    d. clean serial unit/dirty serial unit
    e. connected server unit/disconnected server unit

21. Which two of the following transmission media could a T3 use?
    a. UTP
    b. STP
    c. fiber-optic cable
    d. coaxial cable
    e. microwave
22. Outside of the United States, SONET is known as which of the following?
    a. SNS
    b. SDH
    c. STT
    d. SON
    e. STS
23. Name five factors that you should consider when planning a WAN implementation.
24. What type of equipment is used to convert incoming digital signals from an ISDN line into analog signals for use by an attached telephone?
    a. cable modem
    b. terminal adapter
    c. CSU/DSU
    d. Network Termination 1 (NT1)
    e. Network Termination 2 (NT2)
25. Which transmission medium does SONET use?
    a. coaxial cable
    b. microwave
    c. fiber-optic cable
    d. UTP
    e. STP
26. Why might a company choose to implement a VPN?
    a. to lower its WAN transmission costs
    b. to avoid using an ISP
    c. to increase its WAN security
    d. to increase the reliability of its WAN
    e. to allow remote access for its WAN

27. If you are configuring a Windows 2000 dial-up connection to an ISP, how would you begin to create this connection?
    a. Right-click on the My Network Places icon, choose Properties, choose the Connections tab, then click Make New Connection.
    b. Double-click the My Network Places icon, then double-click the Add Network Place icon.
    c. Click Start, point to Settings, click Network and Dial-up Connections, then double-click the Make New Connection icon.
    d. Right-click the My Computer icon, choose Properties, choose the Network Identification tab, then click Make New Connection.
28. Dial-up connections from a Windows 2000 Professional client will work only with Windows 2000 Remote Access Service (RAS). True or False?
29. For a user running queries on her office LAN's database server from home, which of the following access types makes the most sense?
    a. RAS connection to an ISP
    b. remote control of the database server
    c. Web interface to a domain controller
    d. dial-in VLAN
30. Which of the following is the most popular communications protocol for dial-up networking connections?
    a. SLIP
    b. NCP
    c. LDAP
    d. PPP
    e. RAS

HANDS-ON PROJECTS

For these projects, you will need a Windows 2000 Professional workstation with a working, configured modem, access to a phone line, and a valid ISP account. You will also need a Web browser, such as Internet Explorer or Netscape Communicator, installed on your workstation.

Project 7-1

Because you will probably be both a user of and technical support person for dial-up connections, it is important that you know how to both create and configure them. In this exercise, you will create and configure a dial-up connection to an ISP. Later, you will change some of its parameters to see what happens.

1. Make sure that you have the dial-in parameters (for example, the dial-in number, the name or address of the name server, and what types of protocols the network accepts) specified by your ISP. Usually, these are supplied when you sign up for a dial-in account. They may also be listed in the technical support section of your ISP's Web site. Also make sure that your phone line is plugged into your modem.
2. Click **Start**, point to **Settings**, and then click **Network and Dial-up Connections**. The Network and Dial-up Connections window appears.
3. Double-click the **Make New Connection** icon. The Network Connection Wizard welcome screen appears.
4. If you have not previously configured a dial-up connection on your computer, you will be asked to provide your area code in the Location Information dialog, and then click **OK**. Then you will be asked to provide your location in the Phone and Modem Options dialog and click **OK**. Click **Next** to continue.
5. Choose the second option, **Dial-up to the Internet**, and click **Next** to continue. The Internet Connection Wizard appears with a welcome message, as shown in Figure 7-16.
6. Choose the last option, **I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)**, then click **Next** to continue. You are prompted to indicate how you will connect to the Internet.

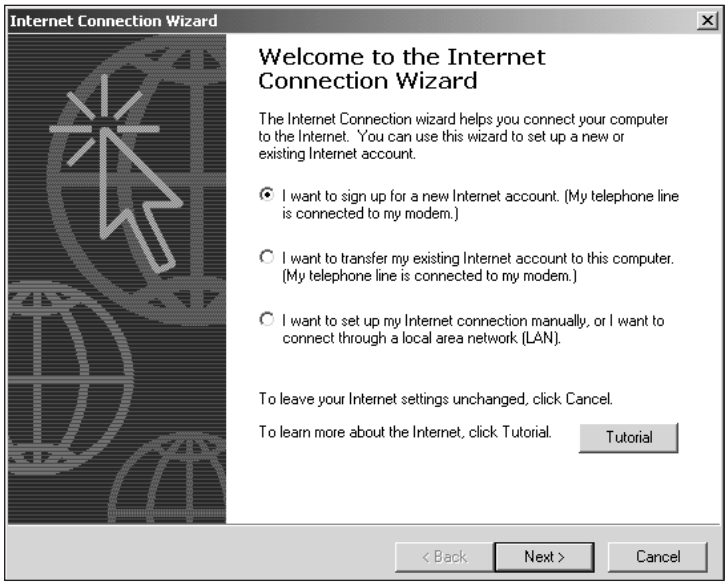

Figure 7-16 The Internet Connection Wizard

7. Choose **I connect through a phone line and modem** (the default), then click **Next** to continue. You are prompted to provide the phone number for your ISP.

8. Type the correct area code and telephone number, and verify that the correct country is selected. For this exercise, you will not need to configure advanced settings. Click **Next** to continue.
9. Provide the user name and password you will use to log into your ISP. This information should have been supplied to you by the ISP. Often the password is case-sensitive, so make sure you type it in correctly and that you don't have the Caps Lock key on. Click **Next** to continue. You are asked to supply a name for this connection.
10. Call this connection TEST, then click **Next** to continue. You are prompted to indicate whether you want to set up an Internet mail account.
11. Choose **No**, then click **Next** to continue. The final screen of the Internet Connection Wizard appears.
12. Click **Finish** to close the wizard and connect to the Internet using your new connection. (Note: if your ISP specifies an unusual configuration for your connection, you may need to adjust the connection's properties before the dial-up connection will work. Do so before continuing to Project 7-2.)
13. If Internet Explorer opens automatically, close it. Disconnect from your ISP.

Project 7-2

Now that you have successfully created an Internet dial-up connection, you will modify some of its parameters to see how configuration changes can affect the connection. This exercise will familiarize you with some of the error messages you might encounter while troubleshooting dial-up networking.

1. Choose **Start**, point to **Settings**, and then click **Control Panel**. The Control Panel window appears.
2. Double-click **Network and Dial-up Connections**. The Network and Dial-up Connections window appears.
3. Right-click the dial-up connection called **TEST**, then choose **Properties** from the drop-down menu. The connection's properties dialog box appears.
4. Select the **Networking** tab.
5. Under "Type of dial-up server I am calling:" choose **SLIP: Unix Connection**.
6. Click **OK** to save your changes and close the properties dialog box.
7. Now try connecting to your ISP using the TEST connection. What happens?
8. Next, you will change another property in the TEST connection configuration. Right-click the dial-up connection called **TEST** in the Network and Dial-up Connections window, then choose **Properties** from the drop-down menu. The connection's properties dialog box appears.

9. Select the **Networking** tab and change the "Type of dial-up server I am calling:" option to **PPP: Windows 95/98/NT 4/2000, Internet**.
10. Under the list of components used by this connection, deselect **Internet Protocol (TCP/IP)**.
11. If NWLink is not already installed, click **Install**. (If NWLink is already installed, skip to Step 13.) The Select Network Component Type dialog box appears.
12. Choose **Protocol**, then click **Add** to continue. The Select Network Protocol dialog box appears.
13. Highlight **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol**, then click **OK**. The NWLink protocol is installed. You will then be returned to the connection's properties dialog box.
14. Click the box next to the **NWLink IPX/SPX/NetBIOS Compatible Transport Protocol** to select it.
15. Click **Close** to save your changes. You return to the Network and Dial-up Connections window.
16. Now double-click the **TEST** icon to make a connection to your ISP. What happens?

Project 7-3

In Chapter 8, you will learn more about Internet networking and, in particular, TCP/IP troubleshooting. One TCP/IP utility, called tracert, allows you to view each node that an Internet connection passes through between your station and the destination you are trying to reach. Even if you aren't troubleshooting a TCP/IP connection, using tracert will help you understand the extent of the Internet's WAN links. For example, you can see how many routers and gateways packets travel through (in other words, how many hops they take) between your workstation and a host far away. For this exercise, you will need a workstation connected to the Internet (either via a dial-up or LAN connection).

1. While connected to the Internet, click **Start**, point to **Programs**, point to **Accessories**, click **Command Prompt**. The Command Prompt window opens.
2. Type **tracert novell.com** at the C:\> prompt, then press **Enter**.
3. Watch the route that your packets take between your computer and the host you have identified. How many nodes do they pass? Can you see the names of long-distance carriers in any of the host names that appear in the route—for example, *mci.net* or *att.net?* Do any of the host names contain acronyms that might give you an idea of what kind of WAN technology the node uses—for example, FDDI or ATM?
4. Try the same exercise with different host names, such as microsoft.com, amazon.com, cisco.com, and npr.org. Do any of your tracert attempts time out? If so, after how many hops?

Project 7-4

If you are asked to recommend software, hardware, or an architecture for WAN links, you will definitely need to know the technologies in greater depth than that provided by this chapter. Even if you are not in that position, however, you will benefit from staying current on WAN technology developments. One of the most interesting evolving fields in WAN technology is the competition between DSL and cable modems for the home user market. In this project, you will find out more about the current state of this contest.

1. Connect to your ISP and open a new browser window.
2. Point your browser to **www.zdnet.com**.
3. In the Search for field, type **DSL** and press **Enter**.
4. Scroll to the bottom of the page until you reach the "Top News and Opinion Items" heading. Click the **See Expanded Results** link to view more titles related to DSL.
5. Choose one article that appears to pertain to DSL technology today and read it. Write a paragraph summarizing its main points.
6. Point your browser to **www.techweb.com**.
7. In the SEARCH field, type **cable modem** and press **Enter**.
8. Choose one article that appears to pertain to the current status of cable modem technology and read it. Write a paragraph summarizing its main points.

CASE PROJECTS

1. A national, nonprofit organization of small business owners called PERKS is holding two simultaneous conferences: one in an Atlanta convention center and one in a Seattle hotel. Both conferences will include speakers, workshops, and exhibit booths showing off new products. The technical manager for PERKS asks for your help in making sure that everything is in order for the conferences. One requirement is having a small LAN established on the exhibit hall floor that will allow visitors to register their names, addresses, and comments. This registration information from attendees at both the Atlanta and Seattle conferences needs to be instantly combined in a single database. What kind of system do you recommend, and why? What additional information might you want to get from the technical manager before you implement anything?
2. A month before the conferences, the technical manager at PERKS decides to add two more hosting locations: Boston and Chicago. The technical manager also wants the keynote speech, which will be delivered at the Boston conference, to be available at the other locations as a live video feed on computers in the exhibit areas. The technical manager wants each of the 15 computers in each location to play the video. How does this new development change your recommendation? What kind of cautionary advice might you give the technical manager about what he is attempting to achieve?

3. You have made the PERKS technical manager a little concerned. Because it is a nonprofit organization, PERKS doesn't have the money to implement the nationwide videoconference solution you proposed. He had no idea how much it would cost. He suggests simply playing the audio portion of the keynote speech on just two computers in each location. From listening to radio broadcasts on the Web, you know that audio files require at least a 56-Kbps connection—but the more throughput, the better. What kind of solution do you recommend now?
4. While the technical manager is out of town at the PERKS conference, he needs to dial from his hotel room to his office's server to pick up his e-mail each night. When he discovers that he can't connect to the server, he calls you for help. The error message he receives says something about not being able to establish a dial-up connection. He uses the Windows 2000 Professional operating system. List the steps you will use to troubleshoot his connection.